

CHAPTER 17

Migrating from Windows 2000 to Windows Server 2003

Windows Server 2003 Migration Overview

In many ways, a migration from Windows 2000 to Windows Server 2003 is more of a service pack upgrade than a major migration scenario. The differences between the operating systems are more evolutionary than revolutionary, and there subsequently are fewer design considerations than in upgrades from the NT 4.0 operating system.

That said, several immediate improvements to the operating system can be realized through migration to Windows Server 2003, whether by migrating all servers immediately or by using a slow, phased approach. Improvements to Active Directory (AD), such as the ability to rename domains and greater scalability, provide incentive for Windows 2000 Active Directory environments to begin migration. Standalone server improvements such as Terminal Services, File and Print Server improvements, Automated Server Recovery, and many more also serve to encourage migrations.

This chapter focuses on the planning, strategy, and logistics of migration from Windows 2000 to Windows Server 2003. In addition, specialized procedures such as using Mixed-Mode Domain Redirect and migrating using the Active Directory Migration Tool (ADMT) are described, and step-by-step instructions complement these processes.

IN THIS CHAPTER

- Windows Server 2003 Migration Overview
- Beginning the Migration Process
- Upgrading a Single Member Server
- Upgrading a Windows 2000 Active Directory Forest
- Upgrading Separate AD Forests to a Single Forest Using Mixed-Mode Domain Redirect
- Consolidating and Migrating Domains Using the Active Directory Migration Tool v2.0
- Consolidating a Windows 2000 Domain to a Windows Server 2003 Domain Using ADMT v2.0
- Best Practices

Beginning the Migration Process

Any migration procedure should define the reasons for migration, steps involved, fallback precautions, and other important factors that can influence the migration process. After finalizing these items, the migration can begin.

Identifying Migration Objectives

Two underlying philosophies influence technology upgrades, each philosophy working against the other. The first is the expression “If it ain’t broke, don’t fix it.” Obviously, if an organization has a functional, easy-to-use, and well-designed Windows 2000 infrastructure, popping in that Windows Server 2003 CD and upgrading may not be so appealing. The second philosophy is something along the lines of “Those who fail to upgrade their technologies perish.”

Choosing between these two philosophies effectively depends on the factors that drive an organization to upgrade. If the organization has critical business needs that can be satisfied by an upgrade, such an upgrade may be in the works. If, however, no critical need exists, it may be wise to wait until the next iteration of Windows or a future service pack for Windows Server 2003.

Establishing Migration Project Phases

After the decision is made to upgrade, a detailed plan of the resources, timeline, scope, and objectives of the project should be outlined. Part of any migration plan requires establishing either an ad hoc project plan or a professionally drawn-up project plan. The migration plan assists the project managers of the migration project accomplish the planned objectives in a timely manner with the correct application of resources.

The following is a condensed description of the standard phases for a migration project:

- **Discovery**—The first portion of a design project should be a discovery, or fact-finding, portion. This section focuses on the analysis of the current environment and documentation of the analysis results. Current network diagrams, server locations, WAN throughputs, server application dependencies, and all other networking components should be detailed as part of the Discovery phase.
- **Design**—The Design portion of a project is straightforward. All key components of the actual migration plan should be documented, and key data from the Discovery phase should be used to draw up Design and Migration documents. The project plan itself would normally be drafted during this phase. Because Windows Server 2003 is not dramatically different from Windows 2000, significant re-engineering of an existing Active Directory environment is not necessary. However, other issues such as server placement, new feature utilization, and changes in AD replication models should be outlined.

- **Prototype**—The Prototype phase of a project involves the essential lab work to test the design assumptions made during the Design phase. The ideal prototype would involve a mock production environment that is migrated from Windows 2000 to Windows Server 2003. For Active Directory, this means creating a production domain controller (DC) and then isolating it in the lab and promoting it to the Operations Master (OM) server in the lab. The Active Directory migration can then be performed without affecting the production environment. Step-by-step procedures for the migration can also be outlined and produced as deliverables for this phase.
- **Pilot**—The Pilot phase, or Proof-of-Concept phase, involves a production “test” of the migration steps, on a limited scale. For example, a noncritical server could be upgraded to Windows Server 2003 in advance of the migration of all other critical network servers. In a slow, phased migration, the Pilot phase would essentially spill into Implementation, as upgrades are performed slowly, one by one.
- **Implementation**—The Implementation portion of the project is the full-blown migration of network functionality or upgrades to the operating system. As previously mentioned, this process can be performed quickly or slowly over time, depending on an organization’s needs. It is subsequently important to make the timeline decisions in the Design phase and incorporate them into the project plan.
- **Training**—Learning the ins and outs of the new functionality that Windows Server 2003 can bring to an environment is essential in realizing the increased productivity and reduced administration that the OS can bring to the environment. Consequently, it is important to include a Training portion into a migration project so that the design objectives can be fully realized.

For more detailed information on the project plan phases of a Windows Server 2003 migration, refer to Chapter 2, “Planning, Prototyping, Migrating, and Deploying Windows Server 2003 Best Practices.”

Comparing the Inplace Upgrade Versus New Hardware Migration Methods

Because the fundamental differences between Windows 2000 and Windows Server 2003 are not significant, the possibility of simply upgrading an existing Windows 2000 infrastructure is an option. Depending on the type of hardware currently in use in a Windows 2000 network, this type of migration strategy becomes an option. Often, however, it is more appealing to simply introduce newer systems into an existing environment and retire the current servers from production. This technique normally has less impact on current environments and can also support fallback more easily.

Determining which migration strategy to use depends on one major factor: the condition of the current hardware environment. If Windows 2000 is taxing the limitations of the

hardware in use, it may be preferable to introduce new servers into an environment and simply retire the old Windows 2000 servers. If, however, the hardware in use for Windows 2000 is newer and more robust, and could conceivably last for another two to three years, it may be easier to simply perform inplace upgrades of the systems in an environment.

In most cases, organizations take a dual approach to migration. Older hardware is replaced by new hardware running Windows Server 2003. Newer Windows 2000 systems are instead upgraded in place to Windows Server 2003. Consequently, auditing all systems to be migrated and determining which ones will be upgraded and which ones retired are important steps in the migration process.

Identifying Migration Strategies: “Big Bang” Versus Slow Transition

As with most technology implementations, there are essentially two approaches in regard to deployment: a quick “Big Bang” approach or a phased, slower approach. The Big Bang option involves the entire Windows 2000 infrastructure being quickly replaced, often over the course of a weekend, with the new Windows Server 2003 environment; whereas the phased approach involves a slow, server-by-server replacement of Windows 2000.

Each approach has its particular advantages and disadvantages, and key factors to Windows Server 2003 should be taken into account before a decision is made. Few Windows Server 2003 components require a redesign of current Windows 2000 design elements. Because the arguments for the Big Bang approach largely revolve around not maintaining two conflicting systems for long periods of time, the similarities between Windows 2000 and Windows Server 2003 make many of these arguments moot. With this point in mind, it is more likely that most organizations will choose to ease into Windows Server 2003, opting instead for the phased migration approach to the upgrade. Because Windows Server 2003 readily fits into a Windows 2000 environment, and vice versa, this option is easily supported.

Migration Options

As previously mentioned, Windows Server 2003 and Windows 2000 “play” together very well. The added advantage to this fact is that there is greater flexibility for different migration options. Unlike migrations from NT 4.0 or non-Microsoft environments, the migration path between these two systems is not rigid, and different approaches can be used successfully to achieve the final objectives desired.

Upgrading a Single Member Server

The direct upgrade approach from Windows 2000 to Windows Server 2003 is the most straightforward approach to migration. An upgrade simply takes any and all settings on a single server and upgrades them to Windows Server 2003. If a Windows 2000 server handles WINS, DNS, and DHCP, the upgrade process will upgrade all WINS, DNS, and DHCP components, as well as the base operating system. This makes this type of migra-

tion very tempting, and it can be extremely effective, as long as all prerequisites described in the following sections are satisfied.

Often, upgrading a single server can be a project in itself. The standalone member servers in an environment are often the workhorses of the network, loaded with a myriad of different applications and critical tools. Performing an upgrade on these servers would be simple if they were used only for file or print duties and if their hardware systems were all up to date. Because this is not always the case, it is important to detail the specifics of each server that is marked for migration.

Verifying Hardware Compatibility

It is critical to test the hardware compatibility of any server that will be directly upgraded to Windows Server 2003. In the middle of the installation process is not the most ideal time to be notified of problems with compatibility between older system components and the drivers required for Windows Server 2003. Subsequently, the hardware in a server should be verified for Windows Server 2003 on the manufacturer's Web site or on Microsoft's Hardware Compatibility List (HCL), currently located at <http://www.microsoft.com/whdc/hcl>.

Microsoft suggests minimum hardware levels on which Windows Server 2003 will run, but it is highly recommended that you install the OS on systems of a much higher caliber because these recommendations do not take into account any application loads, domain controller duties, and so on. The following is a list of Microsoft's recommended hardware levels for Windows Server 2003:

- Intel Pentium III 550MHz CPU or equivalent
- 256MB RAM
- 1.5GB free disk space

That said, it cannot be stressed enough that it is almost always recommended that you exceed these levels to provide for a robust computing environment.

NOTE

One of the most important features that mission-critical servers can have is *redundancy*. Putting the operating system on a mirrored array of disks, for example, is a simple yet effective way of increasing redundancy in an environment.

Verifying Application Readiness

Nothing ruins a migration process like discovering a mission-critical application will not work in the new environment. Subsequently, it is very important to list all applications on a server that will be required in the new environment. Applications that will not be used

or whose functionality is replaced in Windows Server 2003 can be retired and removed from consideration. Likewise, applications that have been verified for Windows Server 2003 can be designated as safe for upgrade. For any other applications that may not be compatible but are necessary, you either need to delegate them to another Windows 2000 server or delay the upgrade of that specific server.

In addition to the applications, the version of the operating system that will be upgraded is an important consideration in the process. A Windows 2000 server install can be upgraded to either Windows Server 2003 Standard Server or Windows Server 2003 Enterprise Server. A Windows 2000 Advanced Server install can be upgraded only to Windows Server 2003 Enterprise Server, however. Finally, only Windows 2000 Datacenter Server edition can be upgraded to Windows Server 2003 Datacenter Server.

Backing Up and Creating a Recovery Process

It is critical that a migration does not cause more harm than good to an environment. Subsequently, we cannot stress enough that a good backup system is essential for quick recovery in the event of upgrade failure. Often, especially with the in-place upgrade scenario, a full system backup is the only way to recover; consequently, it is very important to detail fallback steps in the event of problems.

Upgrading a Standalone Server

After all various considerations regarding applications and hardware compatibility have been thoroughly validated, a standalone server can be upgraded. Follow these steps to upgrade:

1. Insert the Windows Server 2003 CD into the CD-ROM drive of the server to be upgraded.
2. The Welcome page should appear automatically. If not, choose Start, Run and then type **d:\Setup**, where d: is the drive letter for the CD-ROM drive.
3. Click Install Windows Server 2003 (Enterprise Edition).
4. Select Upgrade from the drop-down box, as indicated in Figure 17.1, and click Next to continue.
5. Select I Accept This Agreement at the License screen and click Next to continue.
6. The following screen prompts you to enter the 25-character product key. You can find this number on the CD case or in the license documentation from Microsoft. Enter the product key and click Next to continue.
7. The next screen allows for the download of updated Windows Server 2003 files. They may be downloaded as part of the upgrade or installed later. For this example, select No, Skip This Step and Continue Installing Windows. Then click Next to continue.



FIGURE 17.1 Starting the Windows Server 2003 upgrade.

8. The next prompt is crucial. It indicates which system components are not compatible with Windows Server 2003. It also indicates, for example, that IIS will be disabled as part of the install, as you can see in Figure 17.2. IIS can be re-enabled in the new OS but is turned off for security reasons. Click Next after reviewing these factors.



FIGURE 17.2 Checking the System Compatibility report.

9. The system then copies files and reboots, continuing the upgrade process. After all files are copied, the system is then upgraded to a fully functional install of Windows Server 2003.

NOTE

Many previously enabled components such as IIS are turned off by default in Windows Server 2003. Ensure that one of the post-upgrade tasks performed is an audit of all services so that those disabled components can be re-enabled.

Upgrading a Windows 2000 Active Directory Forest

In many cases, the Windows 2000 environment that will be migrated includes one or many Active Directory domains and forests. Because Active Directory is one of the most important portions of a Microsoft network, it is subsequently one of the most important areas to focus on in a migration process. In addition, many of the improvements made to Windows Server 2003 are directly related to Active Directory, making it even more appealing to migrate this portion of an environment.

The decision to upgrade Active Directory should focus on these key improvement areas. If one or more of the improvements to Active Directory justifies an upgrade, it should be considered. The following list details some of the many changes made to Active Directory in Windows Server 2003:

- **Domain Rename Capability**—Windows Server 2003 Active Directory supports the renaming of either the NetBIOS name or the LDAP/DNS name of an Active Directory domain. The Active Directory rename tool can be used for this purpose, but only in domains that have completely upgraded to Windows Server 2003 domain controllers.
- **Cross-Forest Transitive Trusts**—Windows Server 2003 now supports the implementation of transitive trusts that can be established between separate Active Directory forests. Windows 2000 supported only explicit cross-forest trusts, and the trust structure did not allow for permissions to flow between separate domains in a forest. This limitation has been lifted in Windows Server 2003.
- **Universal Group Caching**—One of the main structural limitations of Active Directory was the need to establish very “chatty” global catalog servers in every site established in a replication topology, or run the risk of extremely slow client login times and directory queries. Windows Server 2003 enables remote domain controllers to cache universal group memberships for users so that each login request does not require the use of a local global catalog server.
- **Inter-Site Topology Generator (ISTG) Improvements**—The ISTG in Windows Server 2003 has been improved to support configurations with extremely large numbers of sites. In addition, the time required to determine site topology has been noticeably improved through the use of a more efficient ISTG algorithm.
- **Multivalued Attribute Replication Improvements**—In Windows 2000, if a universal group changed its membership from 5,000 users to 5,001 users, the entire group membership had to be re-replicated across the entire forest. Windows Server 2003 addresses this problem and allows incremental membership changes to be replicated.
- **Lingering Objects (Zombies) Detection**—Domain controllers that have been out of service for a longer period of time than the Time to Live (TTL) of a deleted object

could theoretically “resurrect” those objects, forcing them to come back to life as zombies, or lingering objects. Windows Server 2003 properly identifies these zombies and prevents them from being replicated to other domain controllers.

- AD-Integrated DNS Zones in Application Partition—Replication of DNS zones has been improved in Windows Server 2003 by storing AD-integrated zones in the application partition of a forest, thus limiting their need to be replicated to all domain controllers and reducing network traffic.

NOTE

For more information on the improvements to Active Directory and the ways they can be used to determine whether your organization should upgrade, refer to Chapter 4, “Active Directory Primer,” Chapter 5, “Designing a Windows Server 2003 Active Directory,” Chapter 6, “Designing Organizational Unit and Group Structure,” and Chapter 7, “Active Directory Infrastructure.”

Migrating Domain Controllers

After the decision is made to migrate the Active Directory environment, it is considered wise to make a plan to upgrade all domain controllers in an environment to Windows Server 2003. Unlike with member servers, the full benefits of the Active Directory improvements in Windows Server 2003 are not fully realized until the entire environment is “Windows Server 2003 functional,” and all DCs are upgraded. With this in mind, a mixed Windows 2000/Windows Server 2003 domain controller environment can be maintained. However, upgrading all domain controllers in an environment to Windows 2000 Service Pack 2 or higher is highly recommended because an issue with replication between domain controllers was first addressed by that service pack.

There are two approaches to migrating domain controllers, similar to the logic used in the “Upgrading a Standalone Server” section. The domain controllers can either be directly upgraded to Windows Server 2003 or replaced by newly introduced Windows Server 2003 domain controllers. The decision to upgrade an existing server largely depends on the hardware of the server in question. The rule of thumb is, if the hardware will support Windows Server 2003 now and for the next two to three years, a server can be directly upgraded. If this is not the case, using new hardware for the migration is preferable.

NOTE

A combined approach can be and is quite commonly used, as indicated in Figure 17.3, to support a scenario in which some hardware is current but other hardware is out-of-date and will be replaced. Either way, the decisions applied to a proper project plan can help to ensure the success of the migration.

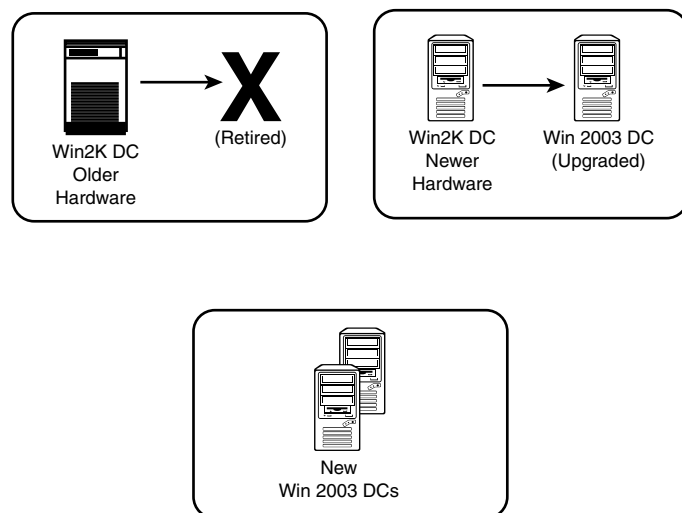


FIGURE 17.3 Combined approach to the upgrade process.

Upgrading the AD Schema Using `adprep`

The introduction of Windows Server 2003 domain controllers into a Windows 2000 Active Directory requires that the core AD database component, the schema, be updated to support the increased functionality. In addition, several other security changes need to be made to prepare a forest for inclusion of Windows Server 2003. The Windows Server 2003 CD includes a command-line utility called `adprep` that will extend the schema to include the extensions required and modify security as needed. `Adprep` requires that both `forest-prep` and `domainprep` be run before the first Windows Server 2003 domain controller can be added.

The Active Directory schema in Windows 2000 is composed of 1,006 attributes, by default, as shown in Figure 17.4. After running `adprep forestprep`, the schema will be extended to include additional attributes that support Windows Server 2003 functionality.

The `Adprep` utility must be run from the Windows Server 2003 CD or copied from its location in the `\i386` folder. The `adprep /forestprep` operation can be run on the server that holds the Schema Master Operations Master (OM) role by following these steps:

1. On the Schema Master domain controller, choose Start, Run. Then type `cmd` and press Enter to open a command prompt.
2. Enter the Windows Server 2003 CD into the CD drive.
3. Where D: is the drive letter for the CD drive, type in `D:\i386\adprep /forestprep` and press Enter.

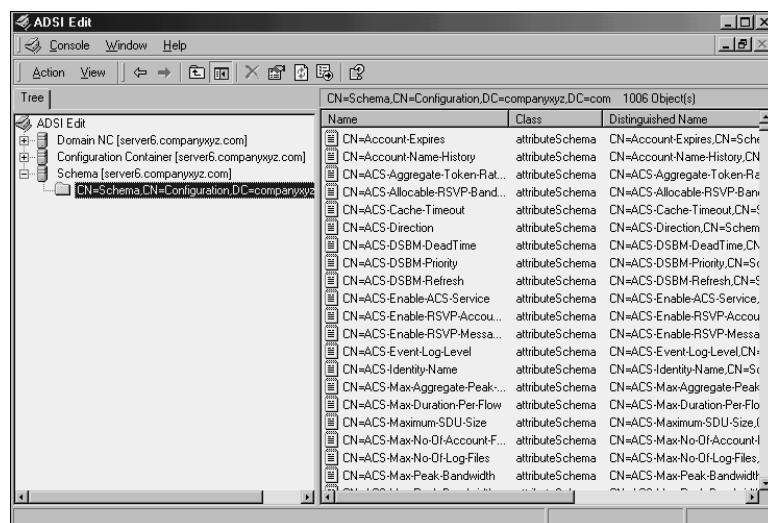


FIGURE 17.4 AD SI Edit before running forestprep.

4. Upon verification that all domain controllers in the AD forest are at Windows 2000 Server Pack 2 or greater, type **C** at the prompt and press Enter.
5. The forestprep procedure extends the Windows 2000 AD schema, as illustrated in Figure 17.5. After the schema is extended, it is replicated to all domain controllers in the forest. Finally, close the command-prompt window.

The Active Directory schema is extended by 244 objects during the forestprep procedure, as illustrated by the low-level directory schema view in Figure 17.6, which shows that the schema now reads at 1,253 objects. After this step is accomplished, the domainprep procedure must be run.

The adprep /domainprep operation must be run once in every domain in a forest. It must be physically invoked on the server that holds the Operations Master (OM) role. The steps for executing the domainprep procedure are as follows:

1. On the Operations Master domain controller, open a command prompt (choose Start, Run, then type **cmd**, and press Enter).
2. Enter the Windows Server 2003 CD into the CD drive.
3. Where D:\ is the CD drive, type **D:\i386\adprep/ domainprep** and press Enter.
4. Type **exit** to close the command prompt window.

```

C:\WINNT\System32\cmd.exe - adprep /forestprep
C:\>d:
D:\>cd i386
D:\i386>adprep /forestprep
ADPREP WARNING: All Windows 2000 domain controllers in the forest should be upgraded to Windows 2000 Service Pack 2 (SP2) or later before performing Windows .NET forest preparation. This must be completed to avoid potential domain controller corruption.
[User Action]
At the command prompt, type C, and then press ENTER to continue, or type any other key and press ENTER to quit.

C
Opened Connection to SERVER6
SSPI Bind succeeded
Current Schema Version is 13
Upgrading schema to version 29
Connecting to "SERVER6"
Logging in as current user using SSPI
Importing directory from file "C:\WINNT\System32\sch14.ldf"
Loading entries.....

```

FIGURE 17.5 Running the adprep forestprep procedure.

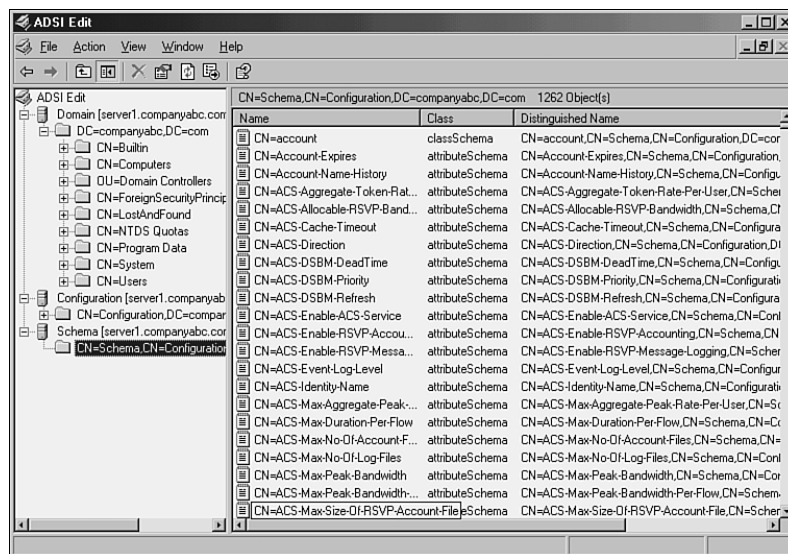


FIGURE 17.6 ADSI Edit after running forestprep.

After the forestprep and domainprep operations are run, the Active Directory forest will be ready for the introduction or upgrade of Windows Server 2003 domain controllers. The schema is extended by 244 attributes and includes support for application partitions. The process of upgrading the domain controllers to Windows Server 2003 can then commence.

NOTE

Any previous extensions made to a Windows 2000 schema, such as those made with Exchange 2000/2003, are not affected by the adprep procedure. This procedure simply adds additional attributes and does not change those that currently exist.

Upgrading Existing Domain Controllers

If the decision has been made to upgrade all or some existing hardware to Windows Server 2003, the process for accomplishing this is straightforward. However, as with the stand-alone server, you need to ensure that the hardware and any additional software components are compatible with Windows Server 2003. After establishing this, the actual migration can occur.

The procedure for upgrading a domain controller to Windows Server 2003 is nearly identical to the procedure outlined in the previous section “Upgrading a Single Member Server.” Essentially, simply insert the CD and upgrade, and an hour or so later the machine will be updated and functioning as a Windows Server 2003 domain controller.

Replacing Existing Domain Controllers

If you need to migrate specific domain controller functionality to the new Active Directory environment but plan to use new hardware, you need to bring new domain controllers into the environment before retiring the old servers. The process for installing a new server is similar to the process in Windows 2000, and the DCPromo utility can be used to promote a server to domain controller status.

Windows Server 2003 supports an enhanced Configure Your Server Wizard, however, which allows an administrator to designate a server into multiple roles. This is the most thorough approach, and the following steps show how to accomplish this to establish a new domain controller in a Windows 2000 Active Directory domain:

1. Open the Configure Your Server Wizard (Start, All Programs, Administrative Tools, Configure Your Server Wizard).
2. Click Next at the Welcome screen, shown in Figure 17.7.



FIGURE 17.7 Configure Your Server Wizard.

3. Verify the preliminary steps and click Next.
4. Select Domain Controller from the list and click Next.
5. Check the settings at the Summary page and click Next.
6. After the AD Installation Wizard is invoked, click Next to continue.
7. At the Operating System Compatibility window, click Next to verify that old versions of Microsoft software such as Windows 95 will not be supported.
8. Select Additional Domain Controller for an Existing Domain and click Next.
9. Type the password of an Administrator account in the AD domain and click Next to continue.
10. Type the domain name into the dialog box of the target AD domain and click Next to continue.
11. Enter a location for the AD database and logs. (You can achieve the best performance if they are stored on separate volumes.) Click Next to continue.
12. Enter a location for the SYSVOL folder. Click Next to continue.
13. Enter a password for Directory Services Restore Mode, which can be used in the event of directory recovery. Click Next to continue.
14. Verify the tasks indicated and click Next to continue. The server then contacts another DC in the domain and replicates domain information, as indicated in Figure 17.8.
15. Click Finish when the process is complete.
16. Click Restart Now when prompted to reboot the domain controller and establish it in its new role in AD.



FIGURE 17.8 Configuring AD.

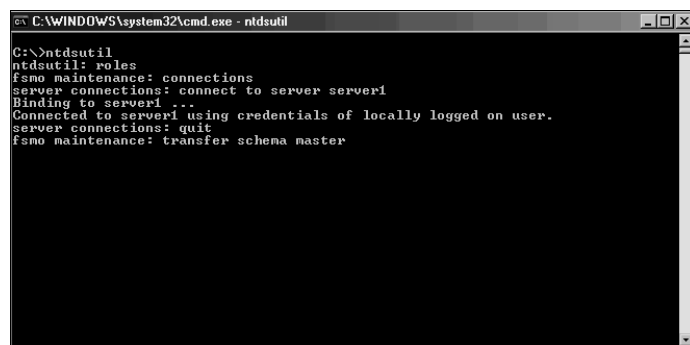
Moving Operation Master Roles

Active Directory sports a multimaster replication model, in which any one server can take over directory functionality, and each domain controller contains a read/write copy of directory objects. There are, however, a few key exceptions to this, in which certain forest-wide functionality must be held by a single domain controller. These exceptions are known as Operation Master (OM) roles, also known as Flexible Single Master Operation (FSMO) roles. There are five OM roles, as follows:

- Schema Master
- Domain Naming Master
- RID Master
- PDC Emulator
- Infrastructure Master

If the server or servers that hold the OM roles are not directly upgraded to Windows Server 2003 but will instead be retired, these OM roles will need to be moved to another server. The best tool for this type of move is the `ntdsutil` command-line utility. Follow these steps using `ntdsutil` to move all OM roles to a single Windows Server 2003 domain controller:

1. Open a command prompt (choose Start, Run and then type `cmd` and press Enter).
2. Type `ntdsutil` and press Enter.
3. Type `roles` and press Enter.
4. Type `connections` and press Enter.
5. Type `connect to server <Servername>`, where `<Servername>` is the name of the target Windows Server 2003 domain controller that will hold the OM roles, and press Enter.
6. Type `quit` and press Enter.
7. Type `transfer schema master`, as shown in Figure 17.9, and press Enter.
8. Click Yes at the prompt asking to confirm the OM change.
9. Type `transfer domain naming master` and press Enter.
10. Click Yes at the prompt asking to confirm the OM change.
11. Type `transfer pdc` and press Enter.
12. Click OK at the prompt asking to confirm the OM change.
13. Type `transfer rid master` and press Enter.



```

C:\WINDOWS\system32\cmd.exe - ntdsutl
C:\>ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server server1
Binding to server1 ...
Connected to server1 using credentials of locally logged on user.
server connections: quit
fsmo maintenance: transfer schema master

```

FIGURE 17.9 Using the ntdsutl utility to transfer OM roles.

14. Click OK at the prompt asking to confirm the OM change.
15. Type **transfer infrastructure master** and press Enter.
16. Click OK at the prompt asking to confirm the OM change.
17. Type **exit** to close the command-prompt window.

Retiring Existing Windows 2000 Domain Controllers

After the entire Windows 2000 domain controller infrastructure is replaced by Windows Server 2003 equivalents and the OM roles are migrated, the process of demoting and removing all down-level domain controllers can begin. The most straightforward and thorough way of removing a domain controller is by demoting them using the dcpromo utility, per the standard Windows 2000 demotion process. After you run the dcpromo command, the domain controller becomes a member server in the domain and can safely be disconnected from the network.

Retiring “Ghost” Windows 2000 Domain Controllers

As is often the case in Active Directory, domain controllers may have been removed from the forest without first being demoted. This may happen due to server failure or problems in the administrative process, but you must remove those servers from the directory before completing an upgrade to Windows Server 2003. Simply deleting the object from Active Directory Sites and Services does not work. Instead, you need to use a low-level directory tool, ADSI Edit, to remove these servers. The following steps outline how to use ADSI Edit to remove these “ghost” domain controllers:

1. Install ADSI Edit from the Support Tools on the Windows Server 2003 CD and open it.
2. Navigate to Configuration\CN=Configuration\CN=Sites\CN=<Sitename>\CN=Servers\CN=<Servername>, where <Sitename> and <Servername> correspond to the location of the ghost domain controller.

- Right-click CN=NTDS Settings and click Delete, as shown in Figure 17.10.

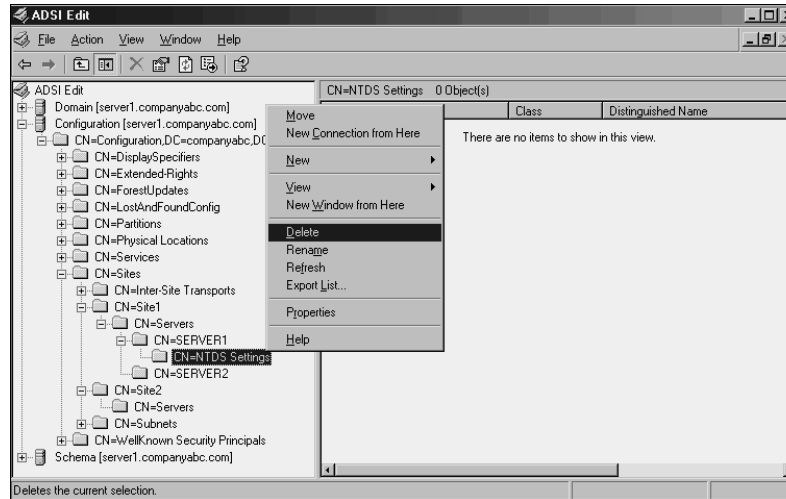


FIGURE 17.10 Deleting ghost domain controllers.

- At the prompt, click Yes to delete the object.
- Close ADSI Edit.

At this point, after the NTDS Settings are deleted, the server can be normally deleted from the Active Directory Sites and Services snap-in.

Upgrading Domain and Forest Functional Levels

Windows Server 2003 does not immediately begin functioning at a native level, even when all domain controllers have been migrated. In fact, a fresh installation of Windows Server 2003 supports domain controllers from Windows NT 4.0, Windows 2000, and Windows Server 2003. You first need to upgrade the functional level of the forest and the domain to Windows Server 2003 before you can realize the advantages of the upgrade.

Windows Server 2003 supports four functional levels. The following levels allow Active Directory to include down-level domain controllers during an upgrade process:

- **Windows 2000 Mixed Domain Functional Level**—When Windows Server 2003 is installed into a Windows 2000 Active Directory forest that is running in Mixed mode, it essentially means that Windows Server 2003 domain controllers can communicate with Windows NT and Windows 2000 domain controllers throughout the forest. This is the most limiting of the functional levels, however, because functionality such as universal groups, group nesting, and enhanced security is absent

from the domain. This is typically a temporary level to run in because it is seen more as a path toward eventual upgrade.

- **Windows 2000 Native Functional Level**—Installed into a Windows 2000 Active Directory that is running in Windows 2000 Native mode, Windows Server 2003 runs itself at a Windows 2000 functional level. Only Windows 2000 and Windows Server 2003 domain controllers can exist in this environment.
- **Interim Level**—Windows Server 2003 Interim mode enables the Windows Server 2003 Active Directory to interoperate with a domain composed of Windows NT 4.0 domain controllers only. Although this is a confusing concept at first, the Windows Server 2003 Interim functional level does serve a purpose. In environments that seek to upgrade directly from NT 4.0 to Windows Server 2003 Active Directory, Interim mode allows Windows Server 2003 to manage large groups more efficiently than if an existing Windows 2000 Active Directory exists. After all NT domain controllers are removed or upgraded, the functional levels can be raised.
- **Windows Server 2003 Functional Level**—The most functional of all the various levels, Windows Server 2003 functionality is the eventual goal of all Windows Server 2003 Active Directory implementations.

After all domain controllers are upgraded or replaced with Windows Server 2003, you can raise the domain and then the forest functional levels by following these steps:

1. Ensure that all domain controllers in the forest are upgraded to Windows Server 2003.
2. Open Active Directory Domains and Trusts from the Administrative Tools.
3. In the left pane, right-click Active Directory Domains and Trusts and then click Raise Domain Functional Level.
4. In the Select an Available Domain Functional Level box, click Windows Server 2003 and then select Raise.
5. Click OK and then OK again to complete the task.
6. Repeat steps 1–5 for all domains in the forest.
7. Perform the same steps on the forest root, except this time click Raise Forest Functional Level in step 3 and follow the prompts, as indicated in Figure 17.11.

NOTE

The decision to raise the forest or domain functional levels is final. Be sure that any Windows 2000 domain controllers do not need to be added anywhere in the forest before performing this procedure. When the forest is Windows Server 2003 functional, this also includes being unable to add any Windows 2000 Active Directory subdomains.

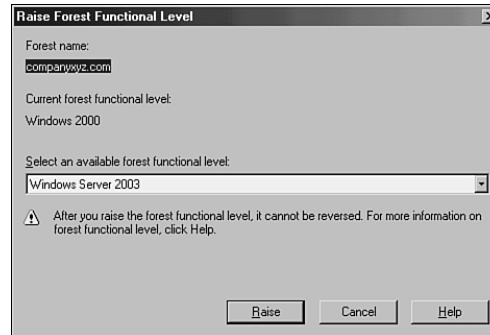


FIGURE 17.11 Raising the forest functional level.

After each domain functional level is raised, as well as the forest functional level, the Active Directory environment is completely upgraded and fully compliant with all the AD improvements made in Windows Server 2003. Functionality on this level opens the environment to features such as schema deactivation, domain rename, domain controller rename, and cross-forest trusts.

Moving AD-Integrated DNS Zones to Application Partition

The final step in a Windows Server 2003 Active Directory upgrade is to move any AD-integrated DNS zones into the newly created application partitions that Windows Server 2003 uses to store DNS information. To accomplish this, follow these steps:

1. Open the DNS Microsoft Management Console snap-in (Start, All Programs, Administrative Tools, DNS).
2. Navigate to DNS*<Servername>*\Forward Lookup Zones.
3. Right-click the zone to be moved and click Properties.
4. Click the Change button to the right of the Replication description.
5. Select either To All DNS Servers in the Active Directory Forest or To All DNS Servers in the Active Directory Domain, depending on the level of replication you want, as shown in Figure 17.12. Click OK when finished.
6. Repeat the process for any other AD-integrated zones.



FIGURE 17.12 Moving AD-integrated zones.

Upgrading Separate AD Forests to a Single Forest Using Mixed-Mode Domain Redirect

Active Directory domains that are running in Windows 2000 Mixed mode can be joined into a separate forest without the need for domain migration tools or workstation reboots. To accomplish this, however, you must run a previously unknown process known as Mixed-Mode Domain Redirect on the environment.

Mixed-Mode Domain Redirect is useful in situations in which branch offices have deployed their own separate Active Directory forests, and the need later surfaces to join these disparate forests into a single, common forest. It is also useful in corporate acquisitions and mergers, where separate forests are suddenly required to merge into a single, unified directory.

Prerequisites and Limitations of the Mixed-Mode Domain Redirect Procedure

The first prerequisite for Mixed-Mode Domain Redirect is that each Active Directory domain in a forest must be running in Windows 2000 Mixed mode. If an organization needs to merge forests but has already gone to Windows 2000 Native mode, other procedures such as using the Active Directory Migration Tool v2.0 or synchronizing directories must be utilized instead.

A big caveat and limitation to this approach is that Windows 2000/XP/2003 clients may already view the domain as an Active Directory domain, requiring themselves to be rejoined to the domain after the operation is complete. Unfortunately, there is no way around this as these client machines eventually discover that their NT domain has become an AD domain, and adjust themselves accordingly. Post-operation, it will become necessary to identify these machines and rejoin them to the new domain structure. This caveat does not hold true for Windows NT 4.0 clients, however.

In addition, this procedure also requires several reboots of existing domain controller servers and is subsequently best performed on a weekend or over a holiday.

Mixed-Mode Domain Redirect Procedure

The concept behind Mixed-Mode Domain Redirect is simple: Take an existing Active Directory domain, downgrade it to a Windows NT 4.0 domain, and upgrade it back into a different environment, as illustrated in Figure 17.13.

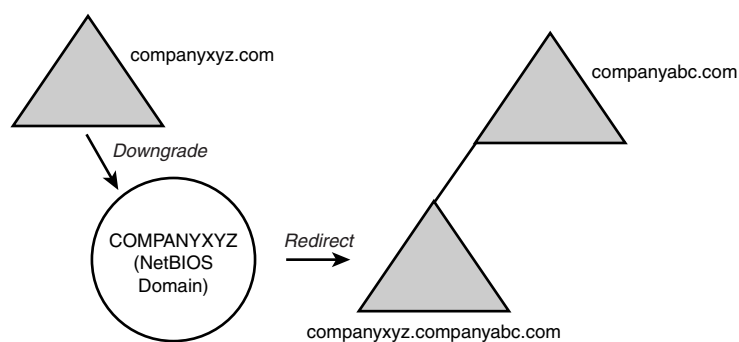


FIGURE 17.13 The Mixed-Mode Domain Redirect procedure.

The example in the diagrams and in the following sections is based on a fictional scenario. You can modify this scenario, however, to include any environment that satisfies the prerequisites outlined previously.

In this scenario, CompanyXYZ has been acquired by CompanyABC, and the need has arisen to merge the CompanyXYZ Windows 2000 forest with the CompanyABC Windows Server 2003 forest. Because the CompanyXYZ domain is running in Windows 2000 Mixed mode, the staff determined that using the Mixed-Mode Domain Redirect procedure would be the most straightforward approach, and there would be no need to change any client settings.

Establishing a Temporary Windows 2000 Domain Controller

The first step in the Mixed-Mode Domain Redirect process is identifying two temporary servers that will be needed in the migration. These servers do not necessarily need to be very fast servers because they will be used only for temporary storage of domain information.

The first temporary server should be set up as a Windows 2000 domain controller in the current Active Directory domain. After the operating system is loaded (Windows 2000 server or Advanced Server), you can run the `dcpromo` command to make it a domain controller in the current domain, per the standard Windows 2000 domain controller upgrade procedure. In addition, this domain controller does not need to be made into a global catalog server.

In our merger scenario, the temporary server SFDCTEMP01 is built with Windows 2000 and Service Pack 3 and added to the `companyxyz.com` Windows 2000 domain, where it becomes a domain controller, as illustrated in Figure 17.14. The current domain controllers—SFDC01, SFDC02, LADC01, and SDDC01—are illustrated as well. These four domain controllers will be migrated to the new environment.

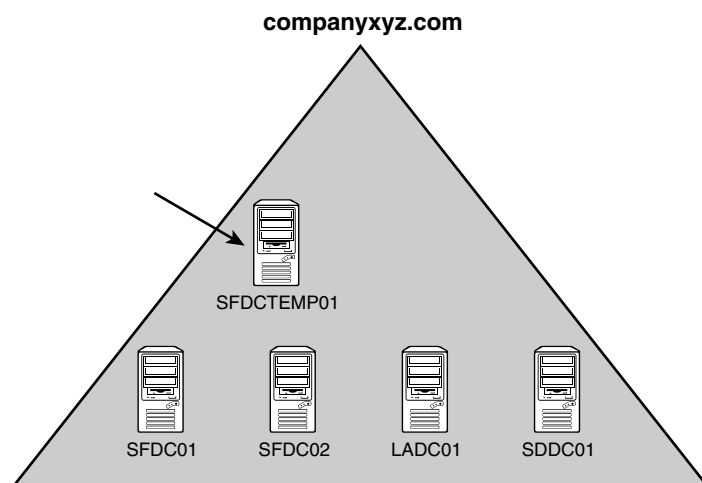


FIGURE 17.14 Establishing a temporary domain controller.

Moving Operations Master Roles and Demoting Existing Domain Controllers

After the new server is introduced to an environment, the five OM roles must be moved from their existing locations and onto the temporary server. This can be done by using the `ntdsutil` utility. The steps to move OM roles were demonstrated previously in the “Moving Operation Master (OM) Roles” section of this chapter.

In the merger example, the schema master and domain naming master OM roles were moved from SFDC01 to SFDCTEMP01, and the OM roles of PDC Emulator, RID Master, and Infrastructure Master were moved from SFDC02 to SFDCTEMP01.

Demoting Production Domain Controllers

Because the old Active Directory forest will be retired, you need to run `dcpromo` on the remaining domain controller servers and demote them from domain controller duties. This effectively makes them member servers in the domain and leaves the only functional domain controller as the temporary server built in the preceding section.

In the merger example, as illustrated in Figure 17.15, SFDC01, SFDC02, LADC01, and SDDC01 are all demoted to member servers, and only SFDCTEMP01 remains as a domain controller.

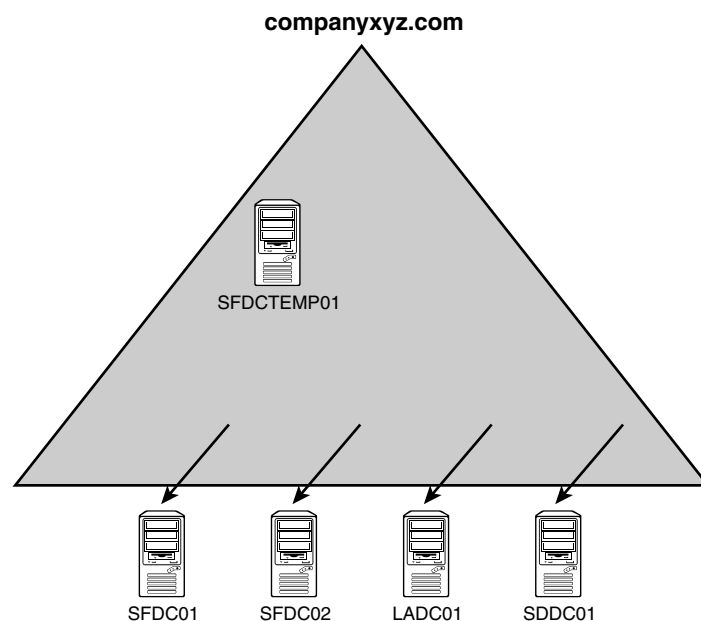


FIGURE 17.15 Demoting production DCs.

Building a Temporary NT 4.0 Domain Controller

An NT Domain Controller will need to be built to allow the procedure to work. It must be brought up as an NT Backup Domain Controller (BDC) for the domain. Because there are no more NT domain controllers, the DC account for the computer must be created on the first temporary domain controller established. The DC account can be created by typing the following at a command prompt:

```
netdom add SFDCTEMP02 /domain:companyxyz.com /DC
```

It is important to note that even though the domain is in Mixed mode, the account must be created in advance if the Primary Domain Controller (PDC) function in the domain runs on a Windows 2000 domain controller; otherwise, the BDC cannot be added to the domain. When the account is established in advance, the second temporary domain controller must be built with Windows NT 4.0 and configured as a BDC in the domain that will be migrated. Because the domain is still in Windows 2000 Mixed mode, NT BDCs are still supported.

In the merger example, the second temporary domain controller is established as SFDCTEMP02 after the computer account is created on SFDCTEMP01 using the `netdom` procedure just described. All existing computer and user accounts are copied into the SAM database on SFDCTEMP02.

Retiring the Existing Forest

The existing Windows 2000 forest can be safely retired by simply turning off the temporary Windows 2000 domain controller. Because this machine controls the OM roles, the Active Directory is effectively shut down. The added advantage of this approach is that you can resurrect the old domain if there are problems with the migration by turning on the first temporary server.

As illustrated in Figure 17.16, the SFDCTEMP01 server is shut off, retiring the companyxyz.com Active Directory domain. However, the COMPANYXYZ NetBIOS domain still exists in the SAM database of SFDCTEMP02, the NT BDC.

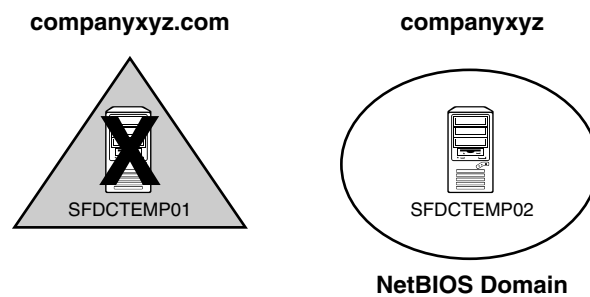


FIGURE 17.16 Retiring the old forest.

Promoting the Second Temporary Server to NT PDC

The NT BDC that you set up then needs to take over as the PDC for the domain, which effectively resurrects the old NetBIOS NT domain structure. This also leaves the domain in a position to be upgraded into an existing Active Directory structure.

In our example, the NT BDC SFDCTEMP02 is promoted to the PDC for the COMPANYXYZ NT domain, preparing it for integration with the companyabc.com Windows Server 2003 domain.

Promoting the NT PDC to Windows Server 2003 and Integrating with the Target Forest

Next, the NT PDC can be promoted to Windows Server 2003 Active Directory. This procedure upgrades all computer and user accounts to Active Directory, and the client settings will not need to be changed.

In the merger example, the Windows Server 2003 CD is inserted into the SCDCTEMP02 server, and a direct upgrade to Windows Server 2003 is performed. As part of the upgrade, the Active Directory Wizard allows the domain to be joined with an existing AD structure. In this case, the CompanyXYZ domain is added as a subdomain to the companyabc.com domain, effectively making it companyxyz.companyabc.com, as illustrated in Figure 17.17.

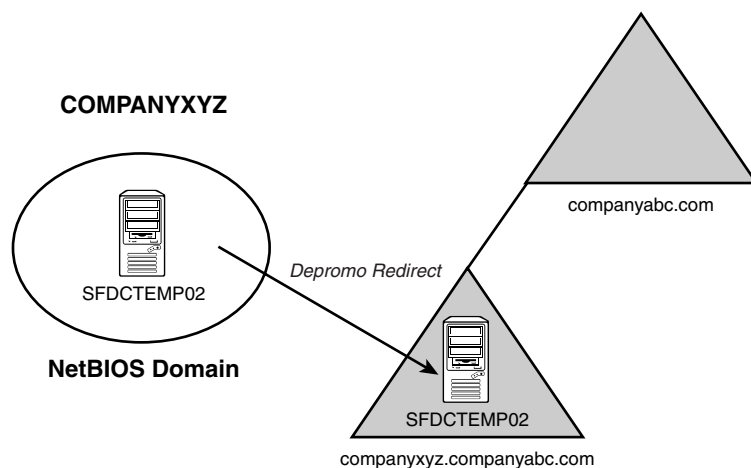


FIGURE 17.17 Redirecting the CompanyXYZ domain to the CompanyABC forest.

Re-establishing Prior Domain Controllers and Moving OM Roles

Another useful feature of this approach is that all the original servers that were domain controllers can be promoted back to their original functions without reloading the operating system. The DCPromo process can be run again on the servers, adding them as domain controllers for the domain in the new forest. In addition, the OM roles can be transferred as previously defined to move the original roles back to their old locations.

In our example, all the original domain controllers that are now member servers in the domain are re-promoted using DCPromo. SFDC01, SFDC02, LADC01, and SDDC01 are all re-added as domain controllers, and the proper OM roles are replaced, as illustrated in Figure 17.17.

Retiring the Temporary Domain Controller

The final step in the Mixed-Mode Domain Redirect is to retire the promoted NT BDC from the domain. The easiest way to accomplish this is to run DCPromo to demote it and then simply shut off the server. Both temporary servers can then be retired from duty and recycled into other uses.

In CompanyXYZ, the SCDCTEMP02 server is demoted using DCPromo and turned off. Overall, the procedure spares the company the need to change client logins, user settings, or server hardware and allows it to re-create the existing Windows 2000 domain within a different Windows Server 2003 Active Directory forest.

Consolidating and Migrating Domains Using the Active Directory Migration Tool v2.0

The development of Windows Server 2003 coincides with improvements in the Active Directory Migration Tool, a fully functional domain migration utility included on the Windows Server 2003 CD. ADMT version 2.0 allows Active Directory and NT domain users, computers, and groups to be consolidated, collapsed, or restructured to fit the design needs of an organization. In regard to Windows 2000 migrations, ADMT v2.0 provides for the flexibility to restructure existing domain environments into new Windows Server 2003 Active Directory environments, keeping security settings, user passwords, and other settings.

Understanding ADMT v2.0 Functionality

ADMT is an effective way to migrate users, groups, and computers from one domain to another. It is robust enough to migrate security permissions and Exchange mailbox domain settings; plus, it supports a rollback procedure in the event of migration problems. ADMT is composed of the following components and functionality:

- **ADMT Migration Wizards**—ADMT includes a series of wizards, each specifically designed to migrate specific components. You can use different wizards to migrate users, groups, computers, service accounts, and trusts.
- **Low Client Impact**—ADMT automatically installs a service on source clients negating the need to manually install client software for the migration. In addition, after the migration is complete, these services are automatically uninstalled.
- **SID History and Security Migrated**—Users can continue to maintain network access to file shares, applications, and other secured network services through migration of the SID History attributes to the new domain. This preserves the extensive security structure of the source domain.
- **Test Migrations and Rollback Functionality**—An extremely useful feature in ADMT v2.0 is the capability to run a mock migration scenario with each migration wizard. This helps to identify any issues that may exist prior to the actual migration work. In addition to this functionality, the most recently performed user, computer, or group migration can be undone, providing for rollback in the event of migration problems.

Consolidating a Windows 2000 Domain to a Windows Server 2003 Domain Using ADMT v2.0

ADMT v2.0 installs very easily but requires a thorough knowledge of the various wizards to be used properly. In addition, best-practice processes should be used when migrating from one domain to another.

The migration example in the following sections describes the most common use of the Active Directory Migration Tool: an interforest migration of domain users, groups, and computers into another domain. This procedure is by no means exclusive, and many other migration techniques can be used to achieve proper results. Subsequently, matching the capabilities of ADMT with the migration needs of an organization is important.

Using ADMT in a Lab Environment

ADMT v2.0 comes with unprecedented rollback capabilities. Not only can each wizard be tested first, but the last wizard transaction can also be rolled back in the event of problems. In addition, it is highly recommended that you reproduce an environment in a lab setting and that the migration process is tested in advance to mitigate potential problems that may arise.

You can develop the most effective lab by creating new domain controllers in the source and target domains and then physically segregating them into a lab network, where they cannot contact the production domain environment. The Operations Master (OM) roles for each domain can then be seized for each domain using the `ntdsutil` utility, which effectively creates exact replicas of all user, group, and computer accounts that can be tested with the ADMT.

ADMT v2.0 Installation Procedure

The ADMT component should be installed on a domain controller in the target domain, where the accounts will be migrated to. To install, follow these steps:

1. Insert the Windows Server 2003 CD into the CD-ROM drive of a domain controller in the target domain.
2. Choose Start, Run. Then type `d:\i386\admt\admigration.msi`, where `d:` is the drive letter for the CD-ROM drive, and press Enter.
3. At the Welcome screen, as illustrated in Figure 17.18, click Next to continue.
4. Accept the end-user license agreement (EULA) and click Next to continue.
5. Accept the default installation path and click Next to continue.
6. When ready to begin the installation, click Next at the next screen.
7. After installation, click Finish to close the wizard.

ADMT Domain Migration Prerequisites

As previously mentioned, the most important prerequisite for migration with ADMT is lab verification. Testing as many aspects of a migration as possible can help to establish the procedures required and identify potential problems before they occur in the production environment.

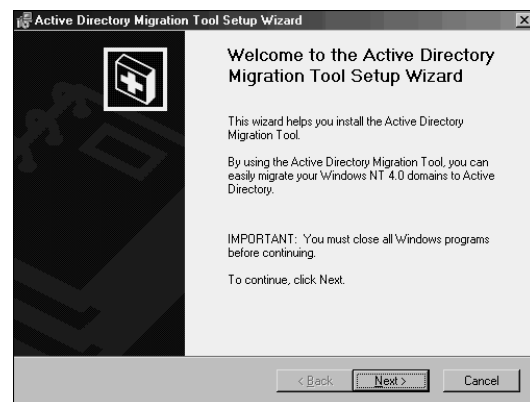


FIGURE 17.18 Installing ADMT.

That said, several functional prerequisites must be met before the ADMT can function properly. Many of these requirements revolve around the migration of passwords and security objects, and are critical for this functionality.

Creating Two-Way Trusts Between Source and Target Domains

The source and target domains must each be able to communicate with each other and share security credentials. Consequently, it is important to establish trusts between the two domains before running the ADMT.

Assigning Proper Permissions on Source Domain and Source Domain Workstations

The account that will run the ADMT in the target domain must be added into the Builtin\Administrators group in the source domain. In addition, each workstation must include this user as a member of the local Administrators group for the computer migration services to be able to function properly. Domain group changes can be easily accomplished, but a large workstation group change must be scripted, or manually accomplished, prior to migration.

Creating Target OU Structure

The destination for user accounts from the source domain must be designated at several points during the ADMT migration process. Establishing an organizational unit (OU) for the source domain accounts can help to simplify and logically organize the new objects. These objects can be moved to other OUs after the migration and this OU collapsed, if you want.

Modifying Default Domain Policy on the Target Domain

Unlike previous versions of Windows operating systems, Windows Server 2003 does not support anonymous users authenticating as the Everyone group. This functionality was designed in such a way as to increase security. However, for ADMT to be able to migrate

the accounts, this functionality must be disabled. When the process is complete, the policies can be reset to the default levels. To change the policies, follow these steps:

1. Open the Domain Security Policy (Start, All Programs, Administrative Tools, Domain Security Policy).
2. Navigate to Security Settings\Local Policies\Security Options.
3. Double-click Network Access: Let Everyone Permissions Apply to Anonymous Users.
4. Check Define This Policy Setting and choose Enabled, as indicated in Figure 17.19. Click OK to finish.



FIGURE 17.19 Modifying the domain security policy.

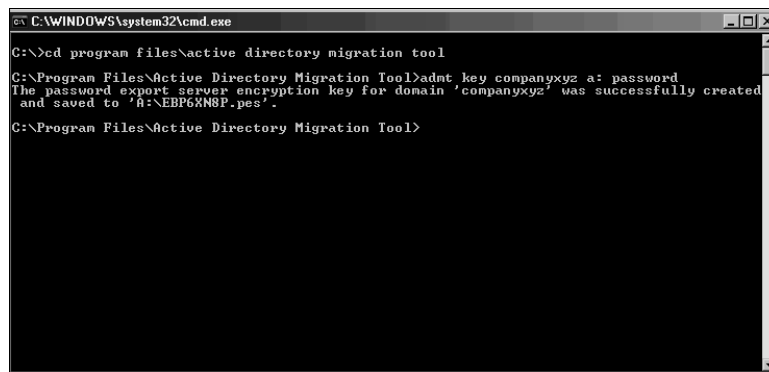
5. Repeat the procedure for the Domain Controller Security Policy snap-in.

Exporting Password Key Information

A 128-bit encrypted password key must be installed from the target domain on a server in the source domain. This key allows for the migration of password and SID History information from one domain to the next.

To create this key, follow these steps from the command prompt of a domain controller in the target domain where ADMT is installed:

1. Insert a floppy disk into the drive to store the key. (The key can be directed to the network but, for security reasons, directing to a floppy is better.)
2. Change to the ADMT directory by typing `cd C:\program files\active directory migration tool` and pressing Enter, where C: is the OS drive.
3. Type `admt key <SourceDomainName> a: <password>`, where `<SourceDomainName>` is the NetBIOS name of the source domain, `a:` is the destination drive for the key, and `<password>` is a password that is used to secure the key. Refer to Figure 17.20 for an example. Then press Enter.



```
C:\WINDOWS\system32\cmd.exe
C:\>cd program files\active directory migration tool
C:\Program Files\Active Directory Migration Tool>admt key companyxyz a: password
The password export server encryption key for domain 'companyxyz' was successfully created
and saved to 'A:\EBP6XN8P.pes'.
C:\Program Files\Active Directory Migration Tool>
```

FIGURE 17.20 Exporting the password key.

4. Upon successful creation of the key, remove the floppy and keep it in a safe place.

Installing a Password Migration DLL on the Source Domain

A special password migration DLL must be installed on a domain controller in the source domain. This machine will become the Password Export Server for the source domain. The following procedure outlines this installation:

1. Insert the floppy disk with the exported key from the target domain into the server's disk drive.
2. Insert the Windows Server 2003 CD into the CD-ROM drive of the domain controller in the source domain where the Registry change will be enacted.
3. Start the Password Migration Utility by choosing Start, Run and typing **d:\i386\ADMT\Pwdmig\Pwdmig.exe**, where d: is the drive letter for the CD-ROM drive.
4. At the Welcome screen, click Next.
5. Enter the location of the key that was created on the target domain; normally, this is the A: floppy drive, as indicated in Figure 17.21. Click Next to continue.
6. Enter the password twice that was set on the target domain and click Next.
7. At the Verification page, click Next to continue.
8. Click Finish after the installation is complete.
9. The system must be restarted, so click Yes when prompted to automatically restart. Upon restarting, the proper settings will be in place to make this server a Password Export Server.



FIGURE 17.21 Setting up the password migration DLL.

Setting Proper Registry Permissions on the Source Domain

The installation of the proper components creates special Registry keys but leaves them disabled by default, for security reasons. You need to enable a specific Registry key to allow passwords to be exported from the Password Export Server. The following procedure outlines the use of the Registry Editor to perform this function:

1. On a domain controller in the source domain, open the Registry Editor (Start, Run, Regedit).
2. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.
3. Double-click the AllowPasswordExport DWORD value.
4. Change the properties from 0 to 1–Hexadecimal.
5. Click OK and close the Registry Editor.
6. Reboot the machine for the Registry changes to be enacted.

At this point in the ADMT process, all prerequisites have been satisfied, and both source and target domains are prepared for the migration.

Migrating Groups

In most cases, the first objects to be migrated into a new domain should be groups. If users are migrated first, their group membership will not transfer over. However, if the groups exist before the users are migrated, they will automatically find their place in the group structure. To migrate groups using ADMT v2.0, use the Group Account Migration Wizard, as follows:

1. Open the ADMT MMC snap-in (Start, All Programs, Administrative Tools, Active Directory Migration Tool).
2. Right-click Active Directory Migration Tool in the left pane and choose Group Account Migration Wizard.
3. Click Next to continue.
4. On the next screen, shown in Figure 17.22, you can choose to test the migration. As mentioned previously, the migration process should be thoroughly tested before actually being placed in production. In this example, however, you want to perform the migration. Choose Migrate Now and click Next to continue.



FIGURE 17.22 Choosing to migrate in the Group Account Migration Wizard.

5. Select the source and destination domains and click Next to continue.
6. On the subsequent screen, you can select the group accounts from the source domain. Select all the groups required by using the Add button and selecting the objects manually. After you select the groups, click Next to continue.
7. Enter the destination OU for the accounts from the source domain by clicking Browse and selecting the OU created in the steps outlined previously. Click Next to continue.
8. On the following screen, there are several options to choose from that determine the nature of the migrated groups. Clicking the Help button details the nature of each setting. In the sample migration, choose the settings shown in Figure 17.23. After choosing the appropriate settings, click Next to continue.
9. If auditing is not enabled on the source domain, you will see the prompt shown in Figure 17.24. It gives you the option to enable auditing, which is required for migration of SID History. Click Yes to continue.



FIGURE 17.23 Setting group options.

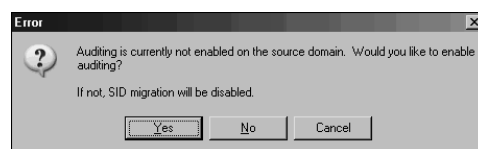


FIGURE 17.24 Enabling auditing.

10. Another prompt may appear if auditing is not enabled on the target domain. Auditing is required for migration of SID History and can be disabled after the migration. Click Yes to enable and continue.
11. A local group named SOURCEDOMAIN\$\$\$ is required on the source domain for migration of SID History. A prompt asking to create this group is displayed at this point, as shown in Figure 17.25, if it was not created beforehand. Click Yes to continue.
12. Another prompt may appear asking to create a Registry key named TcpiClientSupport in the source domain. Once again, this is required for SID History migration. Click Yes to continue.

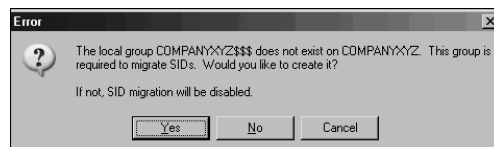


FIGURE 17.25 Creating a local group.

13. If you created the Registry key, an additional prompt then asks whether the PDC in the source domain will require a reboot. In most cases, it will, so click Yes to continue.
14. The next prompt, shown in Figure 17.26, exists solely to stall the process while the reboot of the Source PDC takes place. Wait until the PDC is back online and then click OK to continue.



FIGURE 17.26 Waiting for the source domain PDC reboot.

15. The subsequent screen allows for the exclusion of specific directory-level attributes from migration. If you need to exclude any attributes, they can be set here. In this example, no exclusions are set. Click Next to continue.
16. Enter a user account with proper administrative rights on the source domain on the following screen. Then click Next to continue.
17. Naming conflicts often arise during domain migrations. In addition, different naming conventions may apply in the new environment. The next screen, shown in Figure 17.27, allows for these contingencies. In this example, any conflicting names will have the XYZ- prefix attached to the account names. After defining these settings, click Next to continue.
18. The verification screen is the last wizard screen you see before any changes are made. Once again, make sure that the procedure has been tested before running it because ADMT will henceforth write changes to the Target Windows Server 2003 Active Directory environment. Click Finish when you're ready to begin group migration.
19. The group migration process then commences. Changing the refresh rate, as shown in Figure 17.28, allows for a quicker analysis of the current process. When the procedure is complete, the log can be viewed by clicking View Log. After finishing these steps, click the Close button to end the procedure.

Migrating User Accounts

User accounts are the “bread and butter” of domain objects and are among the most important components. The biggest shortcoming of ADMT v1.0 was its inability to migrate passwords of user objects, which effectively limited its use. However, ADMT v2.0

does an excellent job of migrating users, their passwords, and the security associated with them. To migrate users, follow these steps:

1. Open the ADMT MMC snap-in (Start, All Programs, Administrative Tools, Active Directory Migration Tool).
2. Right-click Active Directory Migration Tool and choose User Account Migration Wizard, as indicated in Figure 17.29.
3. Click Next at the Welcome screen.



FIGURE 17.27 Handling naming conflicts.

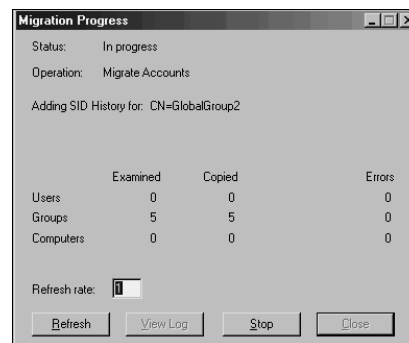


FIGURE 17.28 Altering the migration progress of group accounts.

4. The next screen offers the option to test the migration before actually performing it. As previously mentioned, this process is recommended, so for this example, perform the full migration. Select Migrate Now and then click Next.



FIGURE 17.29 Starting the User Account Migration Wizard.

5. Select the source and target domains in the subsequent screen and click Next to continue.
6. The following screen allows you to choose user accounts for migration. Just click the Add button and select the user accounts to be migrated. After you select all the user accounts, click Next to continue.
7. The next screen, shown in Figure 17.30, allows you to choose a target OU for all created users. Choose the OU by clicking the Browse button. After you select it, click Next to continue.

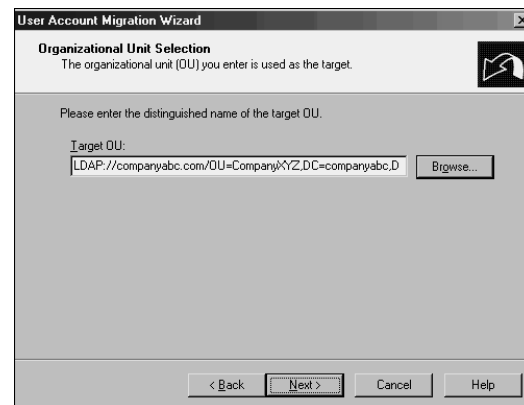


FIGURE 17.30 Selecting the target OU.

8. The new password migration functionality of ADMT v2.0 is enacted through the following screen. Select Migrate Passwords and then select the server in the source domain in which the Password Migration DLL was installed as covered in the

“Installing a Password Migration DLL on the Source Domain” section. Click Next to continue.

NOTE

Depending on if other wizards have already been run, there may be additional steps at this point that happen one time only to set up proper registry settings, reboot DCs, and create special groups. These steps and dialog boxes are documented in steps 9–14 of the “Migrating Groups” section that precedes this section.

9. The subsequent screen deals with security settings in relation to the migrated users. Click Help for an overview of each option. In this example, select the settings as shown in Figure 17.31. Then click Next to continue.

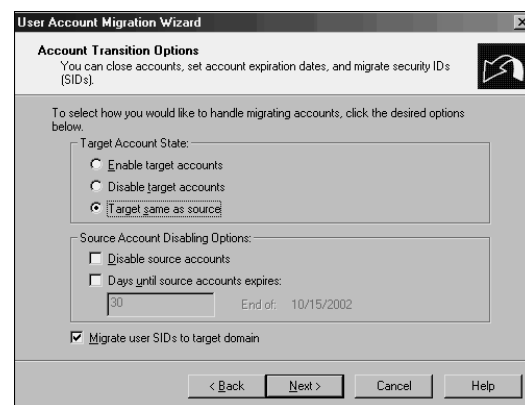


FIGURE 17.31 Setting the account transition options.

10. Enter the username, password, and domain of an account that has Domain Admin rights in the source domain. Click Next to continue.
11. Several migration options are presented as part of the next screen. As before, clicking Help elaborates on some of these features. In this example, select the options as shown in Figure 17.32. Click Next to continue.
12. The next screen is for setting exclusions. Specify any property of the user object that should not be migrated here. In this example, no exclusions are set. Click Next to continue.
13. Naming conflicts for user accounts are common. Designate a procedure for dealing with duplicate accounts in advance and enter such information in the next wizard screen, as shown in Figure 17.33. Select the appropriate options for duplicate accounts and click Next to continue.

14. The following verification screen presents a summary of the procedure that will take place. This is the last screen before changes are written to the target domain. Verify the settings and click Next to continue.
15. The Migration Progress status box displays the migration process as it occurs, indicating the number of successful and unsuccessful accounts created. When the process is complete, review the log by clicking View Log and verify the integrity of the procedure. A sample log file from a user migration is shown in Figure 17.34. Click Close when finished.

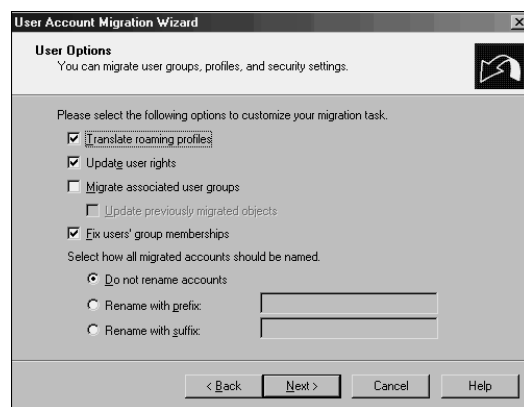


FIGURE 17.32 Setting user options for the User Account Migration Wizard.



FIGURE 17.33 Setting naming conflict settings.

Migrating Computer Accounts

Another important set of objects that must be migrated is also one of the trickier ones. Computer objects must not only be migrated in AD, but they must also be updated at the workstations themselves so that users will be able to log in effectively from their consoles. ADMT seamlessly installs agents on all migrated computer accounts and reboots them, forcing them into their new domain structures. Follow these steps to migrate computer accounts:

```

Migration.log - Notepad
File Edit Format View Help
15:28:48 User91 - Password Copied.
15:28:49 User92 - Password Copied.
15:28:50 User93 - Password Copied.
15:28:51 User94 - Password Copied.
15:28:51 User95 - Password Copied.
15:28:52 User96 - Password Copied.
15:28:53 User97 - Password Copied.
15:28:53 User98 - Password Copied.
15:28:54 User99 - Password Copied.
15:28:54 Processing group membership for CN=XYZ-GlobalGroup1.
15:28:58 LDAP://SERVER1/CN=JuliAnoel,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:58 LDAP://SERVER1/CN=JohnDavis,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:58 LDAP://SERVER1/CN=JamesMills,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:58 LDAP://SERVER1/CN=MarinaNoel,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:58 LDAP://SERVER1/CN=ValLanovsky,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:59 LDAP://SERVER1/CN=,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:59 LDAP://SERVER1/CN=MaryNoel,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:59 LDAP://SERVER1/CN=WayLanDong,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:59 LDAP://SERVER1/CN=GeorgeNoel,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:59 LDAP://SERVER1/CN=ElizabethLanovsky,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:59 LDAP://SERVER1/CN=GeneBondoc,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:59 LDAP://SERVER1/CN=LudmilaMedvedeva,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:59 LDAP://SERVER1/CN=VadimSeFanov,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:59 LDAP://SERVER1/CN=CarrieNoel,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:59 LDAP://SERVER1/CN=ZacharySeFanov,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:59 LDAP://SERVER1/CN=SophieNoel,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:59 LDAP://SERVER1/CN=TanyaSkordina,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:59 LDAP://SERVER1/CN=JosephNoel,OU=CompanyXYZ,DC=companyabc,DC=com added.
15:28:59 LDAP://SERVER1/CN=DavidNoel,OU=CompanyXYZ,DC=companyabc,DC=com added.

```

FIGURE 17.34 Viewing a sample user migration log.

1. Open the ADMT MMC snap-in (Start, All Programs, Administrative Tools, Active Directory Migration Tool).
2. Right-click Active Directory Migration Tool and choose Computer Migration Wizard.
3. Click Next at the Welcome screen.
4. Just as in the previous wizards, the option for testing the migration is given at this point. It is highly recommended that you test the process before migrating computer accounts. In this case, because a full migration will take place, choose Migrate Now. Click Next to continue.
5. Type the names of the source and destination domains in the drop-down boxes on the next screen and click Next to continue.
6. In the following screen, select the computer accounts that will be migrated by clicking the Add button and picking the appropriate accounts. Click Next to continue.
7. Select the OU the computer accounts will be migrated to and click Next to continue.

8. The next screen allows for the option to specify which settings on the local clients will be migrated. Click the Help button for a detailed description of each item. In this example, select all items, as shown in Figure 17.35. Click Next to continue.
9. The subsequent screen prompts to choose whether existing security will be replaced, removed, or added to. In this example, replace the security. Click Next to continue.
10. A prompt then informs you that the user rights translation will be performed in Add mode only. Click OK to continue.
11. The next screen is important. It allows an administrator to specify how many minutes a computer will wait before restarting itself. In addition, you can define the naming convention for the computers, as shown in Figure 17.36. After choosing options, click Next to continue.

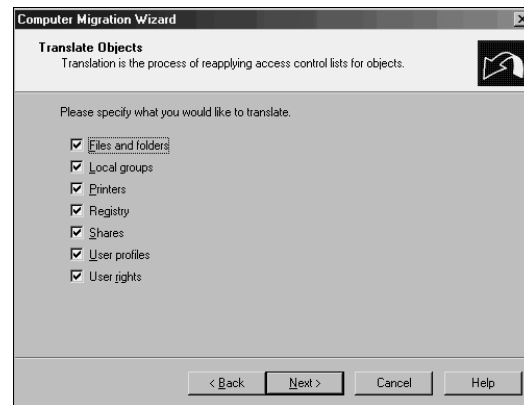


FIGURE 17.35 Specifying objects that will be translated.

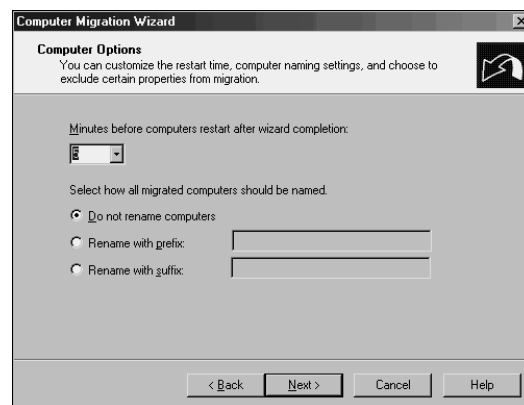


FIGURE 17.36 Selecting computer options.

12. Just as in the previous wizards, exclusions can be set for specific attributes in the following wizard screen. Select any exclusions needed and click Next to continue.
13. Naming conflicts are addressed in the subsequent screen. If any specific naming conventions or conflict resolution settings are required, enter them here. Click Next to continue.
14. The Completion screen lists a summary of the changes that will be made. Review the list and click Finish when ready. All clients that will be upgraded are subsequently rebooted.
15. When the migration process is complete, you can view the Migration log by clicking the View Log button. After verifying all settings, click Close.
16. The client agents are subsequently distributed to all clients that have been migrated. Each agent is installed automatically and counts down until the designated time limit set during the configuration of the Computer Migration Wizard. At that point, the dialog box in Figure 17.37 appears on each workstation.

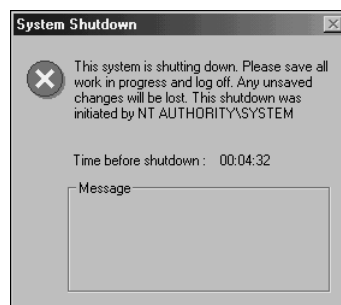


FIGURE 17.37 Notifying users of automatic workstation shutdown.

17. Click Close on the ADMT MMC snap-in to end the wizard.

Migrating Other Domain Functionality

In addition to the Group, User, and Computer Migration Wizards, several other wizards can be used to migrate specific domain-critical components. These wizards operate using the same principles as those described in the preceding sections, and are as straightforward in their operation. The following is a list of the additional wizards included in ADMT v2.0:

- Security Translation Wizard
- Reporting Wizard
- Service Account Migration Wizard

- Exchange Directory Migration Wizard
- Retry Task Wizard
- Trust Migration Wizard
- Group Mapping and Merging Wizard

Virtually all necessary functionality that needs replacing when migrating from one domain to another can be transferred by using ADMT v2.0. It has proven to be a valuable tool that gives administrators an additional option to consider when migrating and restructuring Active Directory environments.

Summary

Although Windows 2000 and Windows Server 2003 are close cousins in the operating system family tree, there are some compelling reasons to upgrade some, if not all, network components. The evolutionary nature of Windows Server 2003 makes performing this procedure more straightforward because the upgrade does not require major changes to Active Directory or operating system design. In addition, advanced procedures and tools such as Mixed-Mode Domain Redirect and ADMT v2.0 provide for a broad range of options to bring organizations to Windows Server 2003 functionality and closer to realizing the benefits that can be obtained through a migration.

Best Practices

- Ensure that one of the post-upgrade tasks performed is an audit of all services so that servers that need IIS have the service re-enabled after migration.
- Because prototype phases of a project are essential to test the design assumptions for a migration or implementation, create a production domain controller and then isolate it in the lab for testing.
- Test the hardware compatibility of any server that will be directly upgraded to Windows Server 2003 against the published Hardware Compatibility List from Microsoft.
- Because the decision to raise the forest or domain functional levels is final, ensure that there is no additional need to add Windows 2000 domain controllers anywhere in the forest before performing this procedure.
- If the server or servers that hold the OM roles are not directly upgraded to Windows Server 2003 but will instead be retired, move these OM roles to another server.
- When using ADMT, migrate groups into a new domain first to keep users' group membership intact.