

Chapter 4: Implementing a Windows 2000 Migration

In Chapter 2, I looked at the choices for developing a migration plan, such as whether to first deploy the Windows 2000 Professional desktops or build the server infrastructure. In this chapter, I'll describe the tools you can use to build your Windows 2000 (Win2K) infrastructure, including moving user and computer accounts and groups to Active Directory (AD).

I recommend moving the server infrastructure to Win2K before moving the user desktops. The main reason for this is that you can use Windows 2000 Server, especially Remote Installation Services (RIS), to deploy the workstations, even though the servers haven't all been upgraded, and you can maintain the production NT network in parallel. You'll most likely have fewer servers to upgrade than workstations, and hopefully the servers have enough horsepower to handle Win2K duties. (For server specifications, see Chapter 1.)

In addition, your Win2K infrastructure, including AD, will aid in the migration because its directory structure gives you more flexibility. This chapter covers the actual process of moving your server infrastructure from NT to Win2K and gives you an outline of the procedures—for both intra-forest domains (domains in the same AD) and inter-forest domains (any domains, anywhere). Whether you decide to follow the in-place upgrade or use a complicated side-by-side approach, I'll describe some complex situations that you may face.

You'll notice that much of this chapter focuses on using the Active Directory Migration Tool (ADMT). The reasons are two-fold. First, ADMT is easily obtainable—you can download it for free. Second, describing a basic tool gives you an idea of what you can do. ADMT has its shortcomings, however, so I'll also point out where you're better off purchasing a more robust migration tool. Most of us would agree that the more robust tools are well worth the money, considering that they're sold on per migrated seat. It's pretty easy to measure the time and cost savings for such a tool when you see how much time it saves you per user or desktop migrated.

Overview of Migration Choices and Scenarios

When you migrate from NT to Win2K, you have a number of choices of how to proceed, as explained in the previous chapters of this book. Your choices range from an in-place migration through an incremental migration to a parallel migration. (A parallel migration is also referred to as *restructuring*; for a full discussion of this type of migration, see "Restructuring" in Chapter 2.) This chapter describes all three types of migration as well as how to perform them.

Assessing Readiness

It's time to begin the hands-on migration. Do you know enough at this point to begin a successful migration? Quite often, readiness is a trade-off between gathering knowledge and building expertise on the one hand and rapidly tackling technological changes on the other. And you *must* make technological changes to keep your company competitive and build business advantage. Are you ready to begin? Or must you begin, ready or not? It's a tough balance to strike, but you'll be ready to begin as long as you've answered some tough questions. The most important one is: What do you expect to achieve? You need to have a clear idea of how to define or measure the success of your migration.

Chapter 1 introduced some of the important benefits to your business of performing an NT-to-Win2K upgrade. As you move into the migration, you'll begin to recognize them. Otherwise, and this is important, much of the upgrade would just be pointless shuffling of user accounts. This isn't intended to be a sales pitch for Win2K; instead, I hope that you and other users in your organization will recognize these benefits and communicate them to the managers or executives who're writing the checks for your migration project.

Here are some of the immediate benefits, which you can use as conversation points when people ask, "How's the migration going?" After all, they're probably not interested in the fascinating details of SIDHistory so much as the cost/benefit ratio of smooth resource continuity for users.

- **AD**—Centralized, hierarchical resource management with flexible account location and policy-based control
- **Name resolution**—Improved name resolution using the integrated Domain Name System (DNS); also improved Windows Internet Name Service (WINS), needed only for "down-level" NT and Win9x clients
- **Remote Installation Services and IntelliMirror**—Software and desktop-computer deployment
- **Group Policy and Group Policy-based Folder Redirection**—Automated computer management and better use of file servers (for relocating the My Documents folder and others)
- **Distributed File System (Dfs) and offline files**—Easier, more unified access to files in "anytime/anywhere mode"
- **Connectivity**—More Routing and Remote Access Service (RRAS) options, including improved security options
- **Terminal services**—They make your life as administrator easier because you'll take fewer trips to the data center or server room. This in turn lowers the company's administrative-support costs.

Gathering Information and Reporting

The more information you can gather, the better prepared you'll be to address the problems listed below. As you'll see from the comparison of ADMT with a full-blown product later in this chapter (see "Domain Migration Administrator"), the products from NetIQ Corporation, BindView Corporation, FastLane Technologies, and Aelita Software Corporation offer more reporting features.

A reporting tool is valuable for finding errors and problems before migration begins. Here is what it should be telling you.

- Problems with group or user names, such as collisions in groups and user account names or not being Win2K-compliant.
- Similarly, invalid server names or not complying with organizational naming standards.
- What service accounts are being used and need to be migrated.

- Finding domain users with administrative rights, a consideration when migrating the Domain Admins group to the new enterprise forest root domain. The previous Domain Admins may need to be downgraded to admins of a specific Organizational Unit (OU) instead.
- Nested groups in native-mode Win2K source domains.
- Server compatibility. Chapter 1 discussed pre-upgrade testing tools. But another issue to mention here are Alpha-processor servers running NT because they cannot be upgraded to Win2K. At least there is a migration path for Alpha-microprocessor computers—even ADMT includes an agent for them.
- An Exchange alias that differs from the NT account name. This will be discussed in more depth in later chapters on Exchange migration, but the basic issue is that if the NT account name doesn't match the alias in Exchange 5.5, and if the original Win2K account was created using the Active Directory Connector (ADC), some migration tools (such as ADMT) create a duplicate Win2K account. This isn't too much of a problem because the Active Directory Account Cleanup Wizard will take care of it. (See "Active Directory Account Cleanup Wizard" later in this chapter.)
- Exchange 5.5–specific information such as public folder permissions, which need to be migrated from mailboxes and distribution lists to Win2K users and groups. You can run the PFAdmin.exe tool from the Exchange 2000 Resource Kit to list the public folder permissions before you start migrating.
- Exchange 5.5 mailboxes that have multiple NT accounts associated with them and NT accounts that have multiple Exchange 5.5 mailboxes. I'll discuss how to deal with this using the NTDSNoMatch utility later, but I mention it now because reporting tools can give you a heads-up for the problems you'll face.

Having a Validated Recovery Plan

I'm quite confident that once you begin the upgrade process and realize some of its benefits, you won't want to go back to your old NT (or other) network. But in case you do, you need to have a contingency plan. Too often I hear the phrase "backup and recovery plan," when all of the emphasis is placed on backup plan and little effort is given to recovery actions. Instead, I stress having a validated recovery plan—backups are meaningless unless they can actually be used to recover from disaster. At each step of the upgrade process, it's important to have a contingency plan that has been validated to prove that it works. I'll point out the high-risk steps where you must heed this advice.

Understanding Active Directory Design

Hopefully, you've planned your migration based on the previous chapters of this book. If you're migrating from a distributed or decentralized security model, the location of the migrated objects in the source domain is very important—and you've hopefully given considerable thought to your use of OUs for the purposes of administrative delegation.

However, even at this point, I must review some fundamentals of AD design. One reason is that you may have skipped the earlier chapters and headed straight for the one where you get to run

setup.exe. The second reason is that some AD design issues will come up during migration, such as Group Policy and defining how many domains you'll need. The AD version of these concepts is very different than the source NT domains and workstations that you're migrating.

Defining Domains

Based on your current design and the information provided in the previous chapters, you have an idea what your domain structure will look like. Here's a quick review to ensure that you don't overlook a few things; you don't want to change the domain structure mid-migration.

Microsoft's official stance has been to plan for a single Win2K domain unless there are sufficient reasons to justify additional domains. There are a number of "sufficient reasons".

- Differing needs in account policies, such as password requirements. But what about companies that are spread out geographically, didn't they use domains in NT 4.0 as replication boundaries? Remember that replication boundaries are what Win2K sites are intended for.
- What about users, groups, and computers that are managed by different administrators, especially at different locations? This is what OUs are for.
- What about a company with thousands and thousands of users, didn't NT have a hard limitation of around 40,000 objects? AD domains have a theoretical limit upward of 17 terabytes for the database, which can hold millions of objects (users, groups, computers, and other resources) per domain.

This is the ideal, or theoretical, view. In reality, you may have to consider additional domains in your migration.

The Protected Root Domain

One design that is gaining favor is the *protected root domain*. In this design, the root AD domain is the placeholder at the top of the forest; all other domains are subordinate, or child, domains. Very few user and machine accounts are placed in the root domain, and certainly few administrators. The goal of this design is to protect access to the schema. Without this design, members of the Domain Admins group can add themselves to the Enterprise Admins group and then be granted access to change the schema. So you may consider creating a minimum of two domains, one at the highest level to provide the most secure AD and others as dictated by the needs I discussed above.

Group Policy

The reason I mention Group Policy in this chapter on migration is simple: If you're using NT 4.0 security policies, and depending on the mix of clients and servers, migrating NT workstations to Windows 2000 Professional and NT servers to Win2K and AD Group Policy will produce varying effects. It's really straightforward and simple when laid out properly, so I've summarized in Table 4.1 the effects of Group Policy on computers during migration to Win2K.

Migration Status	NT Workstation Effective Policy	Windows 2000 Professional Effective Policy
NT domain, some workstations upgraded to Win2K	NT 4.0 System Policy (NTConfig.pol in the Netlogon share: %systemroot%\system32\rep\import\scripts).	NT 4.0 System Policy and Local Group Policy.
Computer account migrated to Win2K AD; user logs on to NT domain	NT 4.0 System Policy.	Computer gets AD Group Policy. User gets no Group Policy or System Policy. To apply policy, use Group Policy to enable System Policy.
User account migrated to Win2K AD; computer still in NT domain	NT 4.0 System Policy from the Win2K AD domain.	Only System Policy is applied, not computer or user Group Policy.
Win2K	NT 4.0 System Policy.	AD Group Policy.

Table 4.1: Effective policy on computers when you migrate to Win2K.

Name Resolution

Of course, your new Win2K AD domain will have DNS name resolution fully implemented and tested. But don't forget WINS in the Win2K domain; it's needed for "down-level" NT and Win9x clients until they're fully migrated. Configure the Win2K servers to register with the WINS servers so that the Win2K servers can be located using WINS even in a routed network.

Migrating Desktops


Finally, you need to determine the impact of domain restructuring and migration on the end user. Will users' desktops be migrated, or will users start fresh with new computers and operating system (OS)? Maintaining the same desktop can be a challenge, and re-creating the desktop can be time-consuming if users do it manually. I'll look at the role of migration tools in desktop migration later in this chapter (see "Migrating Computer Accounts").

In-Place Upgrades

The simplest approach to migrating to Win2K is an *in-place upgrade*. (For a discussion of in-place upgrades, see Chapter 2, "Designing a Migration Strategy.") There are no account collisions or problems to solve, such as what order to migrate groups or accounts in. All accounts in the current domain show up in the new domain. (However, this may not be desirable because you might want to use the opportunity of upgrading to Win2K to clean up those unneeded accounts and groups before the migration begins.) Another advantage of an in-place upgrade may be quicker implementation (usually when you need to upgrade only a few servers and you don't need new hardware).

The primary criterion for choosing between an in-place upgrade and a parallel upgrade (also known as restructuring) is whether you're satisfied with your NT domain structure, including the

fact that the domain name matches the desired DNS domain name. Even if this isn't the case, an in-place upgrade is still possible. The Win2K domain will retain the NT domain name, but you can use user principal name (UPN) logons that match the desired namespace. For example, a logon may be user@company even though the underlying domain is NTDomain1. When you migrate a user to a Win2K domain using a migration tool such as ADMT, the UPN attribute is left blank; however, there is an implicit UPN suffix for every user that matches the current domain name.


 Before upgrading a server to Win2K, check the hardware specifications and the references to the Hardware Compatibility List (HCL) in Chapter 1. The server should be running at least Windows NT 4.0 Service Pack 4.

Synchronizing Domain Controllers

Microsoft has long recommended that before you start an in-place upgrade, you synchronize an NT backup domain controller (BDC) with the primary domain controller (PDC), then remove the BDC from the network. If something goes wrong during the upgrade, you can remove the failed Win2K domain controller, place the NT BDC back on the network, then promote it to PDC to restore your NT domain. However, you must do this within a few days; otherwise, the domain controllers may have resynchronized their passwords and may no longer recognize the old domain controller. Taking the PDC offline will prevent any further changes to domain accounts or groups.

Upgrading to Win2K

You can upgrade existing NT servers to Win2K without affecting the NT domain only if they're member servers, not domain controllers. You can upgrade member servers in any order without affecting the domain. This point has confused a few people who were wary of introducing Win2K into their NT domains. A domain is upgraded when the NT PDC is upgraded to Win2K. When you run the Windows 2000 Server upgrade, the Active Directory Installation Wizard prompts you to choose between joining an existing domain tree or forest and starting a new domain tree or forest.

 Synchronize the domain controllers' accounts databases before beginning migration, then verify that the computer clocks are also in sync.

To use new hardware, install NT, add the new computer as a BDC, promote it to PDC, then upgrade it to Win2K. Whether you judge it to be a silly superstition or a good practice, many people prefer to install a clean copy of Win2K rather than upgrade the OS from NT. Installing a clean copy can prevent inheriting many years' worth of problems and configuration changes. Using the Win2K unattended setup installation process or a drive-imaging program, all partitions are deleted, and new partitions are formatted with NT file system (NTFS). Using this approach, there are really few upgrades. Normally, the next step is to upgrade the BDCs to Win2K, but using the wipe-and-replace approach, you're actually installing fresh domain controllers into the upgraded domain.

Once you've upgraded all BDCs to Win2K, you can make the switch from mixed mode to native mode. This will allow you to use some additional AD features, such as universal groups and group nesting, as well as the cloning tools discussed later in this chapter (see "Account Cloning and Restructuring Tools").

Validating the Process

Before proceeding with the upgrade, it's important to validate the process in a lab environment. This helps detect and prevent problems with the upgrade. For example, third-party software may modify the NT Security Account Manager (SAM) database by inserting strings into attributes that otherwise aren't allowed, causing the migration tools to fail. To validate the upgrade process:

1. Remove a BDC from the production network, start it in the isolated lab, then use the NT Server Manager to promote it to PDC
2. Attach clients to the PDC and validate that accounts can successfully log on and change passwords
3. Upgrade the PDC to Win2K and verify that the clients can successfully log on and change passwords.

Incremental Upgrades

Incremental upgrades, also called *parallel upgrades*, can be much more complex than in-place upgrades; this also means that they can be much more flexible. (For more information on parallel upgrades, also called restructuring, see "Restructuring" in Chapter 2.) In this section, I'll describe *intra-forest migrations*, which occur among domains in the same AD, and *inter-forest migrations*, which occur between NT domains and AD forests. The incremental upgrade process begins when you run DCPromo. This creates the root domain in the first tree of a new forest unless an existing forest is joined.

Namespace Issues

If you're not satisfied with your NT domain structure, including the DNS domain name, you must consider creating a new namespace by building the Win2K AD and migrating resources (users, computers, shares, mailboxes, and so on) to the new domain. A few companies choose an incremental upgrade just so they can maintain a parallel environment and even separate the namespace for their external DNS presence (company.com) from their network (company.net).

Hardware Upgrades

As we've seen, Win2K domain controllers are much more resource-intensive than NT domain controllers. One reason to perform an incremental upgrade is when you introduce new hardware into your environment. True, you can introduce new hardware for an in-place upgrade, as described above, but the parallel path is much safer in circumstances such as evaluating hardware from a new vendor. For example, perhaps you've implemented a new network backbone and the Win2K domain controllers will use Gigabit Ethernet, but the server model and

processor requirements have yet to be determined. If you need to completely redo the Win2K infrastructure, the parallel approach has much less of an impact on a production environment.

SIDs and Re-ACLing

When an NT account is migrated to Win2K AD, it's most helpful if the account can still access resources in the old NT domain. New AD users shouldn't have to supply separate logon credentials to access those old NT file servers. Access to network resources is controlled using Access Control Lists (ACLs), which identify users and groups by their security identifier (SID). You can think of a SID as the NT user account DNA—it provides a unique identification of the account and is used to build the ACLs on each resource to determine who has what type of permissions.

When an account is migrated from one domain to another domain using cloning, a new account is created in the second domain. (Cloning is discussed in detail in “Handling Permissions Issues” in Chapter 3.) The new account may have the same name as the original account, but it definitely has a different SID. A security translation tool such as ADMT is used to create the new SID. The ADMT Security Migration Wizard changes the security descriptors for network resources to refer to the SID for the new account, ensuring that the new account or group has the same access to resources enjoyed by the original user account or group.

This process of changing security descriptors is called *security translation*, or *re-ACLing*. You can do this type of inter-forest migration yourself, but without migration tools, it's horribly inefficient. Everything that the migration tools automate you have to do manually, so I don't give it much coverage as a migration procedure here.

sIDHistory

Another option is to clone the account into the new domain, along with the SID, and keep both accounts active. This is taken care of using *sIDHistory*, which is an attribute on Win2K accounts that contains the NT account's original SID. In Chapter 3, I introduced the concept of SID history, but my odd capitalization of the term reflects the actual representation of the attribute in AD. During migration, both the original account and the newly created account have access to resources based on the same SID. This is ideal because it creates transparency to the end user.

One minor problem is that this opens up a security hole. A cloned account can be used to gain access to a user's information while the user is still using the old account and is unaware of the access violation. (This and other security issues are discussed in more depth in “Security Considerations” later in this chapter.)

Keep in mind that *sIDHistory* is an attribute that is visible to you using ADSI Edit (which replaced the Active Directory Services Viewer), but if you attempt to write the property, it won't let you. The reason for this is to close the security gap that exists if you're able to copy a SID without verifying that you have access to the original SID. Thus, *sIDHistory* can be written only using cloning tools that access the appropriate method or application programming interface (API).

Intra-Forest Migrations

An intra-forest migration involves moving security principals such as users, groups, and computers among domains in the same AD forest. This is the scenario in which NT domains are upgraded and join the Win2K AD forest, and the resources are moved later. The Win2K child domains can be consolidated into one or two AD domains, thus simplifying Group Policy as well as administration of users and groups. ADMT is commonly used for intra-forest migrations, as are third-party tools from BindView Corporation, FastLane Technologies, NetIQ Corporation, and Aelita Software Corporation.


When you perform an intra-forest migration, first migrate resource domains, then migrate account domains. The procedures are detailed below in a checklist that you can use to keep track of the process. These steps are tried and true, and following the order will help you avoid problems that can be caused by re-migrating previously migrated accounts, as described in “User Account Migration” later in this chapter. If you’ve created groups for computer accounts (in addition to the Domain Computers group), migrate those computer accounts before migrating the groups that they belong to; this will prevent their group membership from being lost.

Migrating Resource Domains

Because this is a resource domain, you won’t be migrating users, so the only accounts you’ll migrate are service accounts. To migrate resource domains:

- Log on to the migration computer using credentials with administrator rights in the source domain. Also, ensure that you have administrator rights on source computers so that you can migrate the service accounts.
- Identify services that are configured to run under domain service accounts (as opposed to running under local system authority; this was often the case in NT). Use the ADMT Service Account Migration Wizard, or a third-party tool, and select the appropriate servers to identify service accounts. The migration tool will build a list of the service accounts that need to be migrated, so you can select them when you run the User Migration Wizard.

It’s important not to skip this step because unless you’ve run the Service Account Migration Wizard first, the User Migration Wizard clears the Password Never Expires option. If you skip this step, your service accounts will fail to authenticate because Win2K is expecting users to change their passwords when they log on to the network for the first time.

 ADMT can only do so much when it comes to migrating service accounts. Some applications, including Exchange Server 5.5, use service account configuration that requires configuration using the Registry or the application itself. In this case, you need to manually update the service account settings or use one of the more powerful third-party migration tools.

- Migrate workstations and member servers. The ADMT Computer Migration Wizard installs an agent on each computer being migrated to join the computer to the target domain, then restart the computer. If you have multiple boot options in the c:\boot.ini file, make sure that the Win2K option is the default. When you migrate computers, only accounts from the same domain as the computer account are migrated. If accounts from another domain exist in the local computer's ACLs, you need to translate them manually (for example, using the ADMT Security Translation Wizard). For this reason, you don't need to select any options on the Translate Objects page.
- Migrate the service accounts identified above. A service account may exist in either a master account domain or the same resource domain as the server. If the service account is in the master account domain, select the account domain as the source domain. You can use the ADMT User Migration Wizard to do this.
- Migrate domain local groups. Using the ADMT Group Migration Wizard, on the Group Options page, make sure that Do Not Rename Accounts is the only option selected. Verify that the following events are logged in the target domain security log: event ID 635, Security Enabled Local Group Created, and event ID 636, Security Enabled Local Group Added.
- Decommission the resource domain. Because this section is on intra-forest migrations, you'll only decommission Win2K domains. To properly remove the resource domain, first identify which Win2K domain controllers in the resource domain are holding the Flexible Single-Master Operation (FSMO) roles, then save them for last. Run DCPromo on one of the other domain controllers in the resource domain to launch the Active Directory Installation Wizard, then walk through the guided steps to demote the server so that it's no longer a domain controller.

Once you've demoted each domain controller, it can join the target domain and optionally be promoted to a domain controller in the new domain. When you reach the last domain controller in the resource domain, select the This Server Is the Last Domain Controller in the Domain check box in the Active Directory Installation Wizard.

- Proceed to the next section to migrate intra-forest account domains.

Migrating Account Domains

To migrate account domains:

- Migrate domain global groups using a tool such as the ADMT Group Migration Wizard. When you migrate global groups from a native-mode source domain, in order for the groups to contain members that haven't yet been migrated from the source domain, make the target group type a universal group. Also, when you migrate a distribution group from a Win2K source domain and the target group exists as a security group, even if you select the Replace option, the target group will remain a security group.

- If you're upgrading NT domains as part of the intra-forest migration, prepare to keep login scripts in sync between the NT source domain and the Win2K target domain as you migrate users. (In NT, the source is \\PDC%\systemroot%\system32\repl\export\scripts, while in Win2K, the target is \\ADDC\Sysvol\FQDN\Scripts.) One suggestion is to use the AT command to schedule a nightly Robocopy between these two locations. (Robocopy is described later in "Deployment Tools and Techniques.")
- Migrate users and roaming profiles. If you're using the ADMT User Migration Wizard, on the User Options page, select the Translate Roaming Profiles and Update User Rights check boxes.
- Migrate local profiles. In the ADMT Security Translation Wizard, on the Translate Objects page, select the User Profiles check box; on the Security Translation Options page, select the Add check box.
- Manually migrate the domain controllers and decommission the account domain. (For details, see "Migrating Resource Domains" above.)

Inter-Forest Migrations

Migrating from a Windows NT domain to a Win2K domain is considered inter-forest because the NT domain isn't part of the AD forest. Performing an inter-forest migration has several disadvantages. Without using third-party tools (that is, by using ADMT and not NetIQ's Domain Migration Administrator, described later in this chapter), you cannot copy passwords among forests. An inter-forest migration in this situation requires the user's password to be reset, and the new password must be conveyed to the user somehow; quite often, this opens up a security hole.

Another disadvantage of performing an inter-forest migration when the source domain is Win2K is that Globally unique identifiers (GUIDs) aren't preserved on objects migrated. Objects in AD are identified by GUIDs, which most cloning tools don't preserve. This may be a concern, as I mention later, in preserving user logon profiles, or if you've written applications that rely on these GUIDs to identify objects, because the GUIDs will now be different.

When performing an inter-forest migration, you first migrate account domains, then migrate resource domains. (This is the reverse of intra-forest migrations.)

Migrating Account Domains

To migrate account domains:

- Design and install the Win2K AD and target domain(s). The target domain(s) must be operating in native mode; make the switch using the Active Directory Domains and Trusts MMC snap-in.
- Create two-way trusts among the domains using the Trust Migration Wizard or use the Active Directory Domains and Trusts MMC snap-in to manually create trusts between the source and target domains. Don't use the Trust Migration Wizard to verify existing trusts, only to create new trusts.

- Migrate global groups using a tool such as the ADMT Group Migration Wizard. This tool can take care of group mapping, where a group in the source domain is migrated to a different group in the target domain. Once you run the wizard, the group mapping information is kept in the ADMT database (discussed in more detail later).
- Prepare to keep login scripts in sync between the NT source domain and the Win2K target domain as you migrate users. (In NT, the source is `\\PDC%\systemroot%\system32\repl\export\scripts`, while in Win2K, the target is `\\ADDC\Sysvol\FQDN\Scripts`.) One suggestion is to use the AT command to schedule a nightly Robocopy between these two locations. (Robocopy is described later in “Migration Tools and Techniques.”)
- Migrate a group of test or pilot user accounts and verify their access to resources from the new domain to the old domain. To migrate the accounts, you can use the ADMT User Migration Wizard. Because this is an inter-forest migration, users are prompted to change their passwords when they log on to the network for the first time. Even if the Password Never Expires Option is set on the source account, you must still change the target account’s password.

This might present a problem for service accounts, so be sure to identify service accounts using the ADMT Service Account Migration Wizard; later in this chapter (see “Migrating Service Accounts”), I’ll describe running this wizard to find all of the service accounts in use on all of your servers. What happens when a user logs on with an account that has been flagged to force the password change, but the User Cannot Change Password check box is selected? The user won’t be able to log on until an administrator clears this check box.

- Proceed to the next section to migrate inter-forest resource domains. To ensure that migration goes smoothly, wait until the resource domain migration is complete before you decommission the source account domain. You’ll need a source account domain controller to migrate service accounts, local groups, and workstation profiles.

Migrating Resource Domains

To migrate resource domains:

- Create two-way trusts among the domains using the Trust Migration Wizard or use the Active Directory Domains and Trusts MMC snap-in to manually create trusts between the source and target domain. Use the Trust Migration Wizard to compare and create trusts among the target domain, source domain, *and* all domains that are trusted by the source domain and that contain accounts that are members of local groups that you migrate from the source domain. Don’t use the Trust Migration Wizard to verify pre-existing trusts, only to create new trusts.

- Identify services that are configured to run under domain service accounts (as opposed to running under local system authority; this was often the case in NT). Use the ADMT Service Account Migration Wizard, or a third-party tool, and select the appropriate servers to identify service accounts. The migration tool will build a list of the service accounts that need to be migrated, so you can select them when you run the User Migration Wizard.

It's important not to skip this step because unless you've run the Service Account Migration Wizard first, the User Migration Wizard clears the Password Never Expires option. If you skip this step, your service accounts will fail to authenticate because Win2K is expecting users to change their passwords when they log on to the network for the first time.

- Migrate workstations and member servers. The ADMT Computer Migration Wizard installs an agent on each computer being migrated to join the computer to the target domain, then restart the computer. If you have multiple boot options in the c:\boot.ini file, make sure that the Win2K option is the default. When you migrate computers, only accounts from the same domain as the computer account are migrated. If accounts from another domain exist in the local computer's ACLs, you need to translate them manually (for example, using the ADMT Security Translation Wizard). For this reason, you don't need to select any options on the Translate Objects page.
- Migrate local profiles. Using the ADMT Security Translation Wizard, select the User Profiles check box.
- Migrate shared local groups. Using the ADMT Group Migration Wizard, on the Group Options page, make sure that only Migrate Group SIDs to Target Domain and Do Not Rename Accounts are selected.
- Migrate the service accounts identified above. A service account may exist in either a master account domain or the same resource domain as the server. If the service account is in the master account domain, select the account domain as the source domain. You can use the ADMT User Migration Wizard to do this.
- In the source domain, update service account user rights (typically Logon as a Service and Act As Part of Operating System) for the computers from the source domain. But be sure to select the domain that the service accounts belong to, not the domain that the computer belongs to. Using the ADMT Security Translation Wizard, go to the Translate Objects page and select Local Groups and User Rights.
- Decommission the source domains. Before you remove the domain controllers, remove all trusts between the source resource domain and master account domain, as well as among any other domains.
- Move the domain controllers to the new domain using the following in-place upgrade procedures (you can't use the ADMT Computer Migration Tool to migrate domain controllers): If the source domain is an NT domain, upgrade the domain controllers to Win2K starting with the PDC. This also runs the Active Directory Installation Wizard.

You'll have the option of joining the domain to the existing forest or creating a new one, and the choice is yours. Creating a new forest will have some implications, such as defining new forest-wide FSMO roles. Either way, the domain controllers will be demoted to member servers in the next step.

When the upgrade is complete, run DCPromo and select the option to demote the domain controller to a member server, then join them to the target domain. If the source domain is a Win2K domain, demote the domain controllers and join them to the target domain. After you move each computer, verify that it has access to resources. You can even do this using a script that connects to resources, but it also helps to log in locally and take a look. If there are any problems, you can usually correct them by running the Security Translation Wizard.

- When the migration process is complete, decommission both the source resource domain and master account domain.

Migration Tools and Techniques

Before I describe the utilities that you may find helpful during migration, I want to say a few words about their desired qualities. Table 4.2 provides an overview of directory migration tools, comparing simple account migration tools, complex domain restructuring and modeling tools, and directory synchronization products. Table 4.3 lists migration tools used for domain restructuring as well as some important considerations, such as the scope (intra-forest or inter-forest), whether changes you make can be rolled back, and how user passwords are handled during migration.

Generating Reports Using ADMT

ADMT provides some reports that allow you to evaluate the migration process and watch for the problems listed above. Reports are first generated, collecting information from computers in the domain, then you can view and print them. As with most reports, the information is static, and the reports must be run again to get fresh information.

Packaged reports allow you to generate information on migrated users and groups, migrated computers, expired computers (computer accounts with expired passwords), impact analysis (users and groups affected by computer migration actions), and name conflicts. Oddly enough, just don't try to save the reports to the root folder of any drive other than the boot disk (for example, on D:\); otherwise, you may get an error stating, "Please input a valid directory path." And after you generate a report, it doesn't show until you close and reopen the ADMT console!

Modeling and Rolling Back

An important feature of any migration tool is the ability to perform testing and modeling. For example, ADMT has a test option that allows you to select the migration settings you want, then run the wizard without actually making any changes to your directories or domains. This option is shown in Figure 4.1. You can then review the log files and reports generated to identify and troubleshoot any potential problems before performing the actual migration. In addition, when

you run the actual migration, ADMT gives you the ability to roll back, or undo, the most recently performed user, group, and computer migrations.

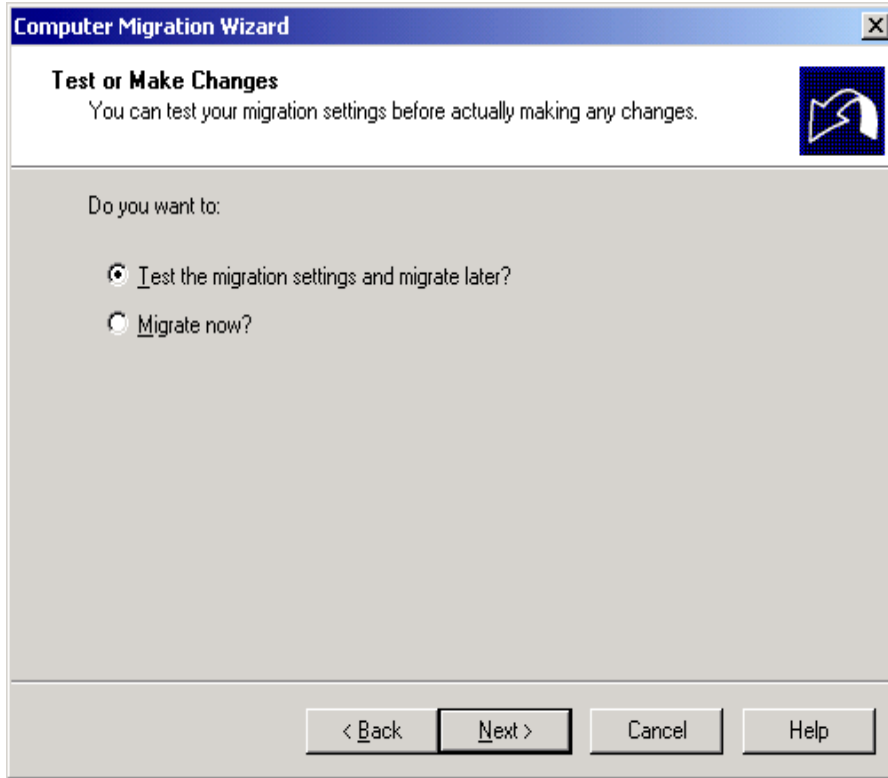



Figure 4.1: ADMT allows you to test migration settings and migrate later.

 There are some exceptions to rolling back. One occurs when you've migrated a user or group and you run the ADMT User or Group Migration wizard again (to pick up any changes to group membership in case there has been a substantial time lag during the migration). If you choose the Replace Conflicting Accounts option, the Undo wizard won't be able to undo these changes.

Directory Migration Tools

Table 4.2 gives an overview of directory migration tools and compares simple account migration tools, complex domain restructuring and modeling tools, and directory synchronization products.

Category	Example	Usage	Location
Basic security principal (users, groups, and computers) migration	Active Directory Migration Tool (ADMT)	Migrate from simple NT configurations (small number of domains) to Win2K AD.	Free download.

Category	Example	Usage	Location
Synchronize Exchange address book with AD in preparation for migration	Active Directory Connector (ADC)	Win2K with Exchange 5.5.	Included with Windows 2000 Server and Exchange 2000.
Complete domain restructuring and modeling of migration scenarios	Products from BindView, FastLane, NetIQ, and Aelita	Migrate from simple NT configurations (small number of domains) to Win2K AD.	Purchase directly from the vendor or through the solution provider performing the migration services.
Inter-forest directory synchronization and management	Microsoft Metadirectory Services (MMS)	Multiple directory management.	Available through the solution provider performing the services.

Table 4.2: Overview of directory migration tools.

Windows 2000 Support Tools


The Windows 2000 Support Tools, located in the Support Tools folder (\SUPPORT\TOOLS) of the Windows 2000 Server CD-ROM, include tools such as:

- **MoveTree**—Allows you to move users, groups, and OUs among Win2K domains in the *same* forest. You can migrate users to a domain and specific OU and restructure later, including all of the Group Policy links to the OU (although there will still be a link to the source domain). You can't move some AD objects among domains, such as computers, and you can't move some objects outside AD, such as profiles, logon scripts, and users' personal data.
- **ClonePrincipal**—Actually a set of scripts and dynamic-link libraries (DLLs) used to clone user and group accounts from a source domain (either an NT domain or a Win2K domain in a separate forest) to a native-mode Win2K target domain. The original account SID is added to the sidHistory of the new account without removing the source account. (This tool is also discussed in "ClonePrincipal" later in this chapter.)
- **SIDWalker**—Allows you to set ACLs on objects that were previously owned by accounts that have been moved, orphaned, or deleted. It consists of two tools, the sidwalk.exe command-line utility and the Security Administration Tools MMC snap-in. SIDWalker is discussed in detail in Chapter 3.

Windows 2000 Server Resource Kit

Nearly 300 tools are included on the Windows 2000 Server Resource Kit companion CD, and some can even be downloaded for free from the URL provided in the tip below. What does the resource kit allow you to do? In addition to helping you with administrative tasks such as managing AD, administering security, working with Group Policy, and automating application deployment, many tools can help you during migration. Here are some examples.

- **Robocopy**—When run with the /sec switch, Robocopy retains NTFS permissions, auditing, and ownership settings during copy and move operations. It also has other useful features, such as the ability to mirror entire directory structures, exclude files that meet certain criteria, and restart canceled copy operations at the point of failure. It's very useful when you want to move file shares from an old server to a new one, but leave files behind that are older than a certain date.
- **GetSid**—Compares account SIDs between a PDC and BDC, which can detect database corruption and save you a lot of grief before you begin an in-place upgrade. (Available as a free download from the URL below.)
- **XcACLs**—Allows you to display and modify the ACL permissions for files and folders contained in a folder (but you cannot print the permissions for files or folders contained in subfolders). You can use XcACLs with ShowACLs, which enumerates access rights for files, folders, and trees. You can also set any file-security option available in Windows Explorer on the command line. These tools are useful for listing ACLs before and after migration and running a comparison to ensure that permissions have migrated properly. (Available as a free download from the URL below.)
- **Addusers**—Allows you to dump a list of users in your NT domain and add the list to a new domain as a comma-delimited text file. However, I feel sorry for anyone who has to resort to this because they have to use XcACLs to restore all permissions!
- **Ntrights**—Grants or revokes Win2K rights to or from users or groups.
- **User State Migration Tool**—Used when upgrading desktops to Win2K. It's actually a set of tools for two processes: ScanState (Scanstate.exe, Shfolder.dll, Sysfiles.inf) and LoadState (Loadstate.exe, Loadras.dll, Usermig.inf). Before migration, you run the ScanState command to collect a user's state information (documents and settings); then after migration, you run the LoadState command to restore the user environment (place the user's state on the Win2K computer).

 You can download the Windows 2000 Server Resource Kit software tools listed on this page for free from: <http://www.microsoft.com/windows2000/library/resources/reskit/tools/default.asp>.

Active Directory Connector

In a nutshell, the Active Directory Connector (ADC) populates the AD with information from an Exchange 5.5 organization (usually in preparation for upgrading to Exchange 2000, although this may be a long-term goal). ADC even enables full two-way synchronization of user, configuration, and distribution-list information between the Exchange 5.5 directory service and Win2K AD. Changes in one location can be scheduled to propagate to the other location. ADC will be discussed in more detail in the chapters on Exchange migration, but it's an essential migration tool, and it's mentioned here because, like ADMT, it can also create Win2K accounts.

Account Cloning and Restructuring Tools

Table 4.3 compares the main migration tools used for domain restructuring and security principal migration.

Tool	Description	Scope	Roll-back*	Effect on Password
Active Directory Migration Tool (ADMT)	Moves users, groups, and computers; migrates trusts; and performs security translation.	Intra-forest or inter-forest.	Yes	Gives the option to preserve passwords only in the same forest. Inter-forest, you must generate new ones.
ClonePrincipal	Clones user and group accounts from an NT or Win2K source domain in a separate forest to a <i>native-mode</i> Win2K target domain.	Among domains in separate forests (inter-forest).	Yes	You must pre-set new initial passwords.
Netdom	Moves computer accounts from an NT or Win2K source domain to a Win2K target domain. Re-creates trusts between domains.	Among domains in the same forest or among separate forests (inter-forest).	No	N/A
MoveTree	Moves users, groups, and OUs among Win2K domains in the same forest.	Among domains in the same forest (intra-forest).	No	Preserves passwords.


*If there is a problem, the tool is non-destructive, leaving the original account intact.

Table 4.3: Migration tools for domain restructuring.

ClonePrincipal

ClonePrincipal is made up of a set of Visual Basic scripts and DLLs (Clonepr.dll, Clone-gg.vbs, Clone-ggu.vbs, Clone-ig.vbs, Clone-pr.vbs, Sidhist.vbs, ADsSecurity.dll, and ADsError.dll). These files clone user and group accounts from a source domain (either an NT domain or a Win2K domain in a separate forest) to a *native-mode* Win2K target domain. The original account SID is added to the sIDHistory of the new account without removing the source account. A sample ClonePrincipal script execution is:

```
cscript clonepr.vbs
```

 When you migrate user accounts using ClonePrincipal and the sample batch files included with it, you may receive an error. The problem is that the tool fails to add the source SID to the destination object's sidHistory. The error will appear as either “The server is unwilling to process the request” or “The source object's SID already exists in destination forest.”

The error occurs because either the built-in accounts in the source domain don't match the target domain or the account has been moved to a different OU—for example, when the built-in Administrator account or the built-in groups are renamed. The error may also occur when you run the ClonePrincipal script for a user account that is already imported but has been moved to a different OU in AD. The solution is to either use a more robust tool to avoid these problems in the first place or rename the problem accounts and groups in either the source domain or the destination domain. After ClonePrincipal has applied the SID history data to the migrated accounts, you can safely rename the built-in accounts and groups.

ADMT

Microsoft worked with Mission Critical Software (now part of NetIQ Corporation) to develop a product that would help some organizations migrate to Win2K native-mode domains. The result is the Active Directory Migration Tool (ADMT), shown in Figure 4.2. You launch ADMT from the Migrator.msc file, not from an executable. ADMT provides a subset of the functionality provided by NetIQ's Domain Migration Administrator, yet even so, ADMT can be crucial to your migration. ADMT is wizard-driven and includes the User Migration, Computer Migration, Group Migration, Service Account Migration, Trust Migration, and Reporting wizards.

The features of ADMT include:

- Wizard-driven with options to just test or perform the migration
- Migration of user accounts, groups, service accounts, computer accounts, and trusts
- Generates a number of reports (described earlier in “Generating Reports Using ADMT”)
- Agents automatically install needed services on source computers
- Group restructuring, mapping, and merging
- Users retain access to resources in both domains at all times during migration.

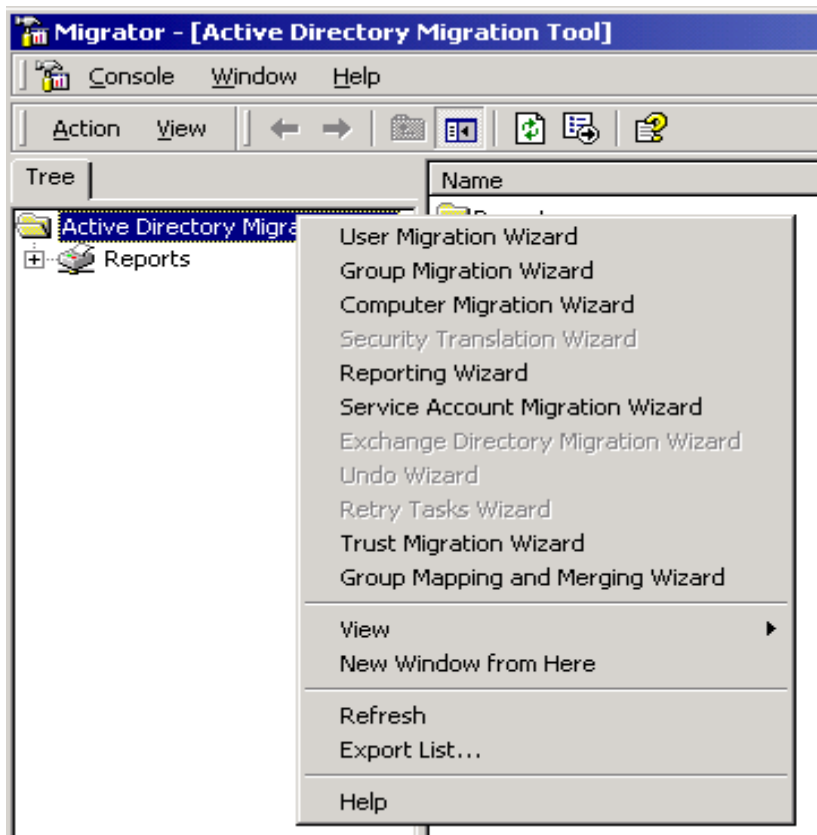



Figure 4.2: Menu options in ADMT.

 You can download ADMT from:
<http://www.microsoft.com/windows2000/downloads/tools/admt/default.asp>.
 This is a redirect from an older location, which you may see published:
<http://www.microsoft.com/NTServer/nts/downloads/other/ADDMT/default.asp>.

Domain Migration Administrator

Because ADMT is free, you just cannot expect as much from it as from Domain Migration Administrator (DMA) from NetIQ Corporation. DMA adds the following functionality to ADMT:

- Third-party vendor support
- The target domain can be NT 4.0 (for additional consolidation with NT domains before migration)
- Additional migration modeling and tracking features
- ActiveScript automation and population of AD from external data sources
- Higher performance for faster enumeration of objects in large domains and re-ACLing of objects

- Migration to Win2K of NetWare, binderies, files, and permissions—just in case you have to migrate from NetWare as well as from NT environments (this interface is shown in Figure 4.3)

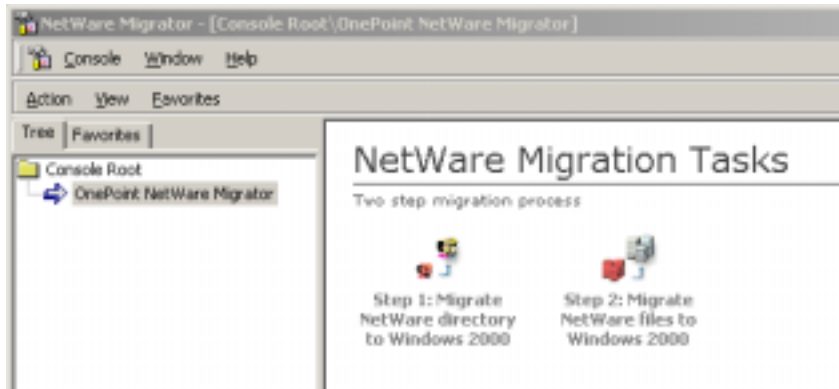


Figure 4.3: Migration of NetWare using DMA.


- More reporting tools, which provide information on cross-domain name collisions, domain relationships, and group memberships
- Model OU structures in your current NT environment. DMA allows you to test an OU structure, then transparently migrate to the same structure in AD. This can be an important benefit because administrators who are new to Win2K can learn and implement AD concepts today and use this knowledge after migration.

NetIQ provides Microsoft Consulting Services (MCS) with DMA, NetIQ NetWare Migrator, and Server Consolidator to use at customer sites to assist in migration. DMA is also made available at reduced cost to solution providers to ensure that they have a more complete toolkit than just ADMT.

ADMT Prerequisites

Because ADMT migrates the NT account SID to the AD sidHistory attribute, you need to switch the destination (Win2K) domain to native mode. The other requirements of ADMT are listed below. The tool handles most of them, but it can't hurt to verify them before beginning or if you run into trouble.

- The PDC of the NT source domain must be Service Pack 4 or higher. The ADMT agent (installed by ADMT on the source computers) can operate on either Intel or Alpha-based computers running Windows NT 3.51 (with SP5), NT 4.0 (SP4 or higher), or Win2K. For the agent to install successfully on computers running Windows 3.51, the ADMIN\$ share must exist.
- The target domain must be running Win2K Service Pack 1 or later and be set to native mode.


 There is another reason to be running Service Pack 1 on Win2K servers. When you clone an NT user object associated with an Exchange Server 5.5 mailbox into a Win2K domain, instead of the user object being properly matched to the NT account, duplicate objects may be created in AD. Exchange 5.5 mailboxes are supposed to be linked to Windows NT accounts by the SID. But ADC was reading the sIDHistory from a Global Catalog (GC) without converting it to hexadecimal format, so it couldn't be compared with the NT account. SP1 fixed this problem.

- Auditing must be enabled on both the target and source domains. On the source domain, enable auditing for the success and failure of user and group management, then enable auditing for the success and failure of account management on the target domain in the Default Domain Controllers policy. If auditing isn't enabled when you run ADMT for the first time, you'll be prompted to have it enabled.
- A DOMAIN group is created in the source domain, and it's used for temporary membership during account migration. This group should have no members. If you're unable to update the sIDHistory for an account and find the account stuck in the DOMAIN\$\$\$ group, remove the account and try the account migration again. (This has frustrated a few people.)
- Add the Domain Admins group from the source domain to the Administrators group in the target domain. Mirror the process and add Domain Admins from the target domain to Administrators in the source domain.
- A functional (verified) trust relationship must exist in both directions. If you've upgraded the domain from NT to Win2K, see the note below.
- ADMT adds a Registry entry (TcpipClientConfig). This is mainly of interest because earlier versions of ADMT required you to set this manually. The latest version will set it for you, or if you're troubleshooting a problem, you can verify that it was set.
- Current logon context: Log on to the computer on which you run ADMT with an account that is Domain Admin in the target domain, a member of the Administrators group in the source domain, and has administrator rights on each computer you migrate.
- Hardware requirements for the computer running ADMT: Add 10 megabytes (MB) to the base Win2K requirements plus 4 kilobytes (K) for each user to be migrated. The disk should have at least 35 MB of disk space free: 7 MB for ADMT and 25 MB for data and log files.

When you upgrade an NT domain to Win2K, ADMT (and ClonePrincipal, for that matter) migrate security principals such as users, groups, and computers, but they don't add the sIDHistory to these objects—that is, the objects are migrated, but the sIDHistory isn't added. This is because trust relationships aren't upgraded. The inbound trust on the source NT domain is considered a “down-level” trust.

Before running ADMT migration, the destination domain performs a version check to see if the source domain is running Win2K so that the Lightweight Directory Access Protocol (LDAP) session can be signed or encrypted. However, the secure LDAP bind between the source and destination domains cannot occur over a “down-level” trust, causing an “Inappropriate Authentication” error message.

The solution is to delete and then rebuild the trust relationship using the Active Directory Domains and Trusts MMC snap-in (or even the Netdom.exe tool if you prefer using the command line). You can use the Trust Migration Wizard to compare trust relationships in the source domain with those in the target domain, and it'll create in the target domain any trust relationships that exist in the source domain.

 When you use ADMT to migrate a user from a Win2K domain to another Win2K domain, an unusual error can prevent migration if all of the domain names in the parent domain of a parent or child domain relationship are in capital letters. In this case, you'll need to use the MoveTree utility to migrate the user. MoveTree allows you to specify both lowercase and uppercase domain names, whereas ADMT doesn't.

ADMT Migration Database

If you look in the folder where you installed ADMT (C:\Program Files\Active Directory Migration Tool is the default location), you'll find a Microsoft Access database named Protar.mdb. While it sounds like an alien or a heavy metal band, it's the database that keeps track of migration status, so it's very important during migration to protect it and keep a backup copy.

This database is designed only for single operations, so if you want multiple administrators to perform migration duties, they need their own copy of ADMT and its associated database. This means that they must coordinate their activities because the state of the migration isn't shared between the two databases. If the ADMT administrator moves to a new computer, he or she will have to manually copy the database to the new location. If you download a newer version of ADMT, be sure to save a copy of Protar.mdb before doing the installation. Verify that the database has upgraded, or you'll have to copy the old database over the newly installed one.

ADMT Logging

ADMT creates the following log files in a Logs folder where the tool is installed:

- **Migration.log**—Records user and group migration
- **Dispatcher.log**—Records the progress of the agent dispatcher
- **Trust.log**—Records the progress of the Trust Migration Wizard

The following log file is stored in the Logs\Agents folder where ADMT is installed:

- **%Computername%.log**—Records the progress of each agent (named after the computer being migrated)


This log file is stored in the folder specified by the %TEMP% variable on the computer to which an agent is dispatched:

- **Dctlog.txt**—Records the agent process on the computer

The level of logging detail is controlled by the Registry entry that controls the logging level. Verbose logging mode is set by changing the value of the logging Registry key to 7:

```
HKEY_LOCAL_MACHINE\Software\Mission Critical  
Software\DomainAdmin\TranslationLogLevel
```

Be forewarned that this will create very large log files, either where ADMT is installed or in the %TEMP% location, as explained above.

 Before you take on the risk of editing the Registry, make sure that you can recover in case you make a mistake. Otherwise, you might prevent the OS from starting.

Using the Migration Tools


This section walks you through using tools such as ADMT to migrate user accounts, groups, service accounts, and computer accounts. Some of the examples also apply to the other, more robust migration tools that you can buy from vendors because they provide more flexibility and more options. Also, I'll give you some tips and tricks, and gotchas, specifically for ADMT in case you decide to stick with it until you find the one feature that it lacks (and then look at purchasing one of the other tools).

Migrating User Accounts

You launch the User Migration Wizard from the menu shown in Figure 4.2. ADMT creates an account in AD based on the entries in the NT SAM database. The Win2K account won't have much information filled in; it will be filled in later from the Exchange 5.5 directory when you run ADC. ADMT doesn't allow source objects to be a built-in account (such as local Administrators, Users, or Power Users). Built-in account SIDs are identical in every domain, so when they exist elsewhere in the forest, they're prevented from being added to SIDHistory.

 During the migration process, ADMT truncates user account names longer than 20 characters.

During migration, ADMT checks the source domain global groups against its list of migrated groups. If the user account in the source domain belongs to an existing group, the user is simply added to the target domain group.

 ADMT operates in additive mode; that is, it adds rights to existing users and groups in the target domain and doesn't remove them. If you're migrating a large number of user accounts at once, the impact on your network can be substantial because the User Migration Wizard retrieves the list of users. Consider performing this migration during off-business hours and close to the network segment of the source domain.

This won't apply to all of you, but if your company has started using the Manager and Direct Report properties, be sure to maintain the relationship by migrating all related users at the same time. For a property to be updated, the Manager's or Direct Report's Win2K account must exist; otherwise, there wouldn't be an account to insert into that field.

User Profile Migration

One of the most frustrating things from the end-users' point of view is architectural changes to the domain structure that mess up their desktops. The ADMT Security Translation Wizard assists in preventing this problem by migrating the user profile. (For details on what else it does, see "The Security Translation Wizard" later in this chapter.)

When you migrate user accounts between two Win2K domains, if a user has already logged on to a computer in the AD forest, it isn't necessary to migrate the user profile. This is because Win2K AD keeps track of the user profile using a GUID for each user account. When you create a new Win2K domain and log on, the user profile is matched using the GUID. When the user logs on, there is no profile for the user account on that computer, so AD matches the GUID with the original profile and associates it with the new user account, keeping the original profile.

Otherwise, you can use the ADMT Security Translation Wizard for inter-forest migrations, where you have to manually keep the user profile consistent. For example, perhaps you store your users' roaming profiles in their home directory on a file serve; if so, the path to the profile is maintained during the migration.

User Migration Options


Table 4.4 lists the options available when you use ADMT to migrate users. Some options are self-explanatory, but there are a few things to know when using others.

This Option	Does This
Translate Roaming Profiles	Copies the roaming profile for the user from the source domain to the target domain. Associates the roaming user profile with the new user account in the target domain.
Update User Rights	Matches the user rights in the target domain to the user rights for the migrated user account from the source domain.
Migrate Associated User Groups	Maintains group membership by migrating any groups that have migrated user accounts as members.
Update Previously Migrated Objects	Updates the groups that have accounts which you select to migrate as members, even if those members were previously migrated. (Available only when the Migrate Associated User Groups check box is selected.)
Do Not Rename Accounts	Uses the same name as the source account unless a naming conflict occurs. (In this case, it follows the options specified on the Naming Conflicts page.)
Rename with Prefix	Adds a prefix that you specify to the name of each migrated group. (This doesn't affect the account in the target domain.)
Rename with Suffix	As above, except that it appends a suffix that you specify.

Table 4.4: Options available in the ADMT User Migration Wizard.

One of the options when using the User Migration Wizard is Replace Conflicting Accounts. This option can come in handy when you rerun the migration tools for a user who has been previously migrated. But it has a side effect that you should know about: It can make changes to the group membership of the target user account. If the original source account has been added to any additional groups, that group membership will be reflected in the new target account. In this


sense, the Replace Conflicting Accounts option actually merges information to the target account. To prevent this from happening, if you're running the User Migration Wizard again, delete the user account from the target domain.

 If your user migration fails and you're left staring at the error message "The selected OU doesn't exist in the target domain"—even though you're 100 percent sure that the OU exists—it could be a known issue with ADMT. If the target OU has a path longer than 520 characters, the User Migration Wizard will fail. To see the full path, you can export the path using the LDIF Directory Synchronization Bulk Import/Export tool (Ldifde.exe) or run ADSI Edit, which allows you to browse the structure of AD. The path will look something like this.

```
LDAP://ou=ReallyLongSubOUName,ou=ReallyLongOUName,  
dc=ReallyLongChildDomainName,dc=ReallyLongParentDomainName,dc=com
```

Because ADMT isn't able to migrate accounts and keep the same passwords across forests, you must generate new passwords for migrated accounts. ADMT can generate passwords that meet minimum-length requirements and meet complexity rules such as: must contain at least three lowercase letters, three uppercase letters, three numbers, and three symbols. (For more migration options, see "Group Migration Options" later in this chapter.)

However, a generated password *must* comply with the password-complexity rules in the target domain. If not, ADMT disables the migrated user account. An administrator must enable the account, and the user will need to choose a password that meets the domain security policy. Successfully generated passwords are logged in a text file. This file may also store computer passwords, so be sure to secure its location.

 If you have user accounts that use characters from the double-byte character set, don't select the Same As the User Name password option; Win2K doesn't accept passwords that contain double-byte characters.


Using ADMT and ADC: Chicken or Egg?

You can use both ADMT and ADC to create user accounts in AD based on NT SAM or the Exchange 5.5 directory, respectively. So you may wonder which one to use, and if you use both, in which order. As long as an NT user account name matches the Exchange alias, there isn't an issue because both tools map the Exchange mailbox information and the NT account information to the same AD account. However, the order of processing does make a difference when an NT user account name doesn't match the Exchange alias. This mismatch is quite common. For example, some organizations might have used information other than account name for populating the alias field, such as employee badge number, or even let the administrator creating the mailbox decide what information to use.

When you run ADMT (or more advanced tools such as NetIQ DMA) first, the account is created in AD. You can then run ADC synchronization, which will match the Exchange mailbox to the account in AD. The problem occurs when you run the tools in the reverse order. When the ADC runs first, it looks in the Exchange 5.5 directory at the alias attribute and creates an account in AD. When ADMT is run next, the name field doesn't match, and a new object is created in AD,

which in this case is a disabled user account. You then need to run the Active Directory Account Cleanup Wizard.

One good thing to say about migration tools like ADMT is that when you migrate a user, group, or computer account, if the object in the target domain already has some information entered in a particular property field (for example, from the ADC) and the object in the source domain doesn't have a value for that property, the information in the target domain will be preserved. In other words, if the information in the source domain field is blank, the migration won't cause the information in the target domain to be lost.

-  You may run into an odd circumstance where you cannot delete a user account after migration. Specifically, if you clone the account using ADMT, then add the user to a local group in Win2K, the account cannot be deleted. You can solve this problem in one of three ways:
1. Use the net command: `net localgroup "localgroupname" NT4Domain\Username" /delete.`
 2. Disconnect the computer from the network, then delete the user account from the Local group using the Computer Management MMC snap-in.
 3. Use the user manager for domains (Usmgr.exe). However, this requires modifying a Registry key. Before proceeding, see Microsoft Knowledge Base article [Q278693](#) for the full Registry key modification and well-advised warnings on editing the Registry.

Let's move from the "chicken or egg" question to group nesting. (Sorry, couldn't resist!) If you're migrating from a native-mode Win2K source domain, you'll want to verify whether group nesting is being used. If it is, you should migrate the accounts in the nested groups using the Group Migration Wizard instead of the User Migration Wizard. The User Migration Wizard doesn't recursively migrate users and nested groups, but does the Group Migration Wizard.

It's probably not too likely that you're already using delegated administration of user accounts, but if you are, be aware that permissions set on a source account in a Win2K domain aren't migrated to the target Win2K domain; they're reset to the defaults. Thus, if you've set the ACL so that only a few administrators or groups of administrators can modify certain user accounts, you'll need to redo that work. This is just a current limitation of ADMT, but if it affects your migration plans, consider purchasing a migration tool that doesn't have this limitation.


Migrating Groups

You can migrate groups using two ADMT wizards: Group Mapping and Merging and Group Migration. The Group Mapping and Merging Wizard allows you to map a group in the source domain to a new or existing group in the target domain. When group members are migrated from the source to the target domain, group memberships reflect the new location. You can also merge multiple groups into one group. ADMT is aware of AD OUs, so it lets you select the target OU for migrated users, groups, and computers.

When you perform an intra-forest migration among Win2K domains in the same forest using ADMT and migrate global groups from a native-mode source domain, the groups are created in the target domain as universal groups instead of global groups. This is because universal groups, unlike global groups, can contain members from the source domain that haven't yet been migrated. Universal groups can contain members from any Win2K domain in the forest.

Selecting the Copy Group Members option allows you to create universal groups immediately because you're copying the accounts instead of moving them.

If the global group source is a mixed-mode domain instead, the global group is copied without sIDHistory instead of being moved. Because global groups cannot contain members from other domains, if you move the global group instead of copying it, the group members are orphaned. When you later migrate the accounts in the groups, group membership is restored, but you must run the Security Translation Wizard to translate sIDHistory.

 You can migrate an NT global group to a Win2K domain local group, but there is a trick: You need to change the group to a universal group as an intermediate step. When you migrate the NT group, it shows up in Win2K as a global group. Change it to a universal group, click Apply, then change the group type to a domain local group. For more information on the reasons for using each group type, see *The Definitive Guide to Windows 2000 Administration* by Sean Daily and Darren Mar-Elia (Realtimerepublishers.com). You'll find a link to this book at: <http://www.realtimerepublishers.com>.

Group Migration Options

Table 4.5 lists the options available when you migrate group members. Some options are straightforward, but others have a few caveats.

This Option	Does This
Generate Complex Passwords	Generates a complex password for each migrated user account and logs it to the file specified by the New Password Output File option.
Set Password to User Name	If you select New Password Output File, logs the passwords. (Each password matches the account name up to the first 14 characters.)
New Password Output File	Specifies the file where assigned or generated passwords are logged.
Disable Source Accounts	Prevents using an old account in the source domain.
Disable Target Accounts	Prevents using a new account in the target domain.
Leave Both Accounts Active	Allows either account to be used to log in to the target or source domain. (See "Security Considerations" later in this chapter.)
Days Until Source Account Expires	Allows you to specify an expiration date for the source account. This option is useful because it forces the transition and eliminates using the old account. (The account expires at midnight at the end of the date you select.)
Translate Roaming Profiles	Copies the roaming profile from the source domain to the target domain and associates the profile with the new user account.

Table 4.5: Migration options for group members.

Group Options

Table 4.6 lists the options you can specify when you migrate groups using ADMT.

This Option	Does This
Update User Rights	Keeps the user rights assigned in the target domain the same as in the source domain.

This Option	Does This
Copy Group Members	Allows you to maintain group membership in the target domain by copying the members from the source domain. (Not available in the Group Merging and Mapping Wizard.)
Update Previously Migrated Objects	Updates the members of groups you select to migrate, even if those members were previously migrated. (Only available if you select the Copy Group Members check box. Not available in the Group Merging and Mapping Wizard.)
Migrate Group SIDs to Target Domain	Adds the SID of the migrated user accounts and groups from the source domain to the SIDHistory of the new accounts and groups in the target domain using a secure connection to the source domain controller.
Do Not Rename Accounts	Uses the same name as the source group unless a naming conflict occurs. (In this case, it follows the options specified on the Naming Conflicts page.)
Rename with Prefix	Adds a prefix that you specify to the name of each migrated group. (Doesn't affect the group in the target domain.)
Rename with Suffix	As above, except that it appends a suffix that you specify.

Table 4.6: Migration options for groups.

I want to mention one last thing about complex, multiple-domain migrations. When you migrate a group from a source to a target domain, consider what happens to groups in a third domain that reference the original group. Of course, a group in the third domain still refers to the original group in the source domain, but if this is an intra-forest migration, the original source group no longer exists. When you migrate the third domain to the target Win2K domain, security references are maintained, and group memberships are properly updated.

Migrating Service Accounts

When ADMT translates security on resources, it installs services (called *agents*) on the source computers. This frees you from manually loading software on the source computers to perform the migration. When an agent's task is completed, it's automatically uninstalled. Keep in mind that when you run the ADMT Service Account Migration Wizard, the account you use must have Logon Locally rights to the remote computer on which the agent is run. Also, if you have an active connection with conflicting credentials from your computer to a resource (usually a printer or a mapped drive) on the computer you're attempting to migrate, the agent won't even dispatch.

After you migrate service accounts, be sure to check the migration log file for errors. If you don't have sufficient rights to update the Service Control Manager on the remote computer, the service account will be migrated to the target domain, but the service configuration on the remote computer won't be updated to use the new service account in the target domain. To fix the problem, change the Service Control Manager access rights on the remote computer and run the Service Account Migration Wizard again, this time selecting the No, Use the Previously Collected Information option.

The Service Account Migration Wizard is designed to handle operations specific to service accounts, such as setting a complex password for the target account, giving the target account Logon As Service rights, clearing the User Must Change Password at Next Logon flag, and

updating each service enumerated by the Service Account Migration Wizard to use the account name and password of the target account.



During migration, this wizard truncates service account names that are longer than 20 characters.

Watch out for UPN! No, this isn't a plug for a television network. It's a warning about a service account listed in UPN format in the Service Account Migration Information report after you run the Service Account Migration Wizard. A service account that is listed in UPN format won't be recognized by the User Migration Wizard as a service account and will thus be treated like a normal user. The workaround is to run the Service Account Migration Wizard and manually specify each domain. (See the caution below about using ADMT to migrate the Exchange 5.5 service account to AD.)

If you allow ADMT to set the switch for User Must Change Password at Next Logon, you'll have to change the password back to the original. The migration administrator must also know the Exchange 5.5 service account password. Using an incorrect password can put Exchange 5.5 servers at risk (of going offline), so I recommend that you don't migrate the Exchange 5.5 service account using ADMT, but use ADC instead.



When you use ADMT to migrate an Exchange 5.5 service account from an NT domain to Win2K, you may find that you're unable to restart the Exchange services. This happens if ADMT sets the service account with the User Must Change Password at Next Logon flag; it also resets the password. To correct this, use the AD Users and Computers MMC snap-in to reset the password to the original, then clear the User Must Change Password at Next Logon check box.

The Security Translation Wizard

The ADMT Security Translation Wizard, shown in Figure 4.4, allows you to update service account rights and migrate local profiles on workstations and member servers. Migrating profiles was discussed in "Migrating User Accounts" earlier in this chapter; now let's look at translating security for service accounts.



Figure 4.4: Security translation options.


When translating security, there are three modes of operation: Replace, Add, and Remove.

- **Replace**—Modifies ACLs with the SID for the account in the target domain instead of the original SID for the account from the source domain. The new account in the target domain receives the same permissions on the selected objects as the original account in the source domain had, but the original account no longer has any permissions.
- **Add**—Puts the SID for the new account in the ACL so that both accounts have the same permissions on the selected objects.
- **Remove**—Strips out the SID so that neither account has permissions.

Here are a few things to keep in mind when translating security.

- When you migrate an account intra-forest, the sidHistory is migrated and the source object is deleted, so the Security Translation Wizard works only in Replace mode.
- If the ADMT Security Translation Wizard cannot resolve a SID to a match in the target domain, it won't modify any permission on the account in the source domain.


- You don't need to translate security on source accounts before deleting them. If you delete the source accounts first, the ACL on resources will show "Account Unknown" because it cannot resolve the SID on the object to an account. You merely need to keep things neat and clean during transition. It's entirely up to you or your migration team whether to translate security before deleting migrated source accounts. As long as resource access is working with the new accounts, you can delete the source accounts. The impact will merely be cosmetic—if you open an ACL properties dialog box, you'll see a list of unknown accounts. Once you upgrade a resource domain to Win2K, the sIDHistory will resolve, and the name will display properly.
- There is a problem with running security translation on Registry key ACLs in Add mode. If the Security Translation Wizard finds more than 15 access control entries (ACEs), it skips the translation and logs an error. This prevents more than 30 ACEs from being added to the Registry key ACL because Win2K can access only the first 30. Any additional users are denied access. This isn't an issue in Replace or Remove mode.

 Before you migrate a user profile, have the user empty the Recycle Bin. This helps to avoid a "Recycle Bin corrupted" error when you use the ADMT Security Translation Wizard. If you see the error, you can just disregard it, but emptying the Recycle Bin can prevent it in the first place.

Migrating Computer Accounts

When you use the Computer Migration Wizard to migrate computer accounts, ADMT installs services (called *agents*) on the source computers. This frees you from manually loading software on the source computers to perform the migration. When an agent's task is completed, it's automatically uninstalled. If you're performing an intra-forest migration, the migrated computer source account isn't disabled or deleted, so you must do it manually or use another tool to automate that task.

You can use third-party tools to update a computer remotely, change its domain membership, and restart it as needed. They can upgrade both servers and workstations. But what about users who've upgraded their workstations themselves and are ready to join your new domain? By default, Win2K grants the Add Workstations to Domain privilege to the Authenticated Users group. This means that authenticated users can bypass the ACL check and add up to a predefined number of machine accounts, which by default is set to 10.

 For information on creating a group for the purpose of restricting who can join computers to your domain, see Microsoft Knowledge Base article [Q238793](#). For information on changing the default limit for the number of computers that an authenticated user can join to a domain, see [Q251335](#).

Oddly enough, you can rename NT computers during migration but not Win2K computers. (The wizard allows you to append a prefix or suffix to a Win2K computer name, but it doesn't rename the computer. Instead, it leaves the computer in the source domain and logs an error.) You can rename NT computers before or after migration, but you must do it manually. When you rename them by adding a prefix, make sure that the machine names remain unique; otherwise, you'll only successfully migrate the first account. For example, using a prefix of NTRESDOM leaves

you only seven characters out of the 15-character NETBIOS machine name, so SQLSERVER1 and SQLSERVER2 will duke it out to be the first NTRESDOMSQLSERV.

For migrated Win2K computers, the Pre-Windows 2000 Computer Name field in AD is reset to the default value. Because this field represents only the first 14 characters of the computer name, you must again watch out for conflicts.

The types of objects that you can migrate using the Computer Migration Wizard are shown in Figure 4.5. I've found that if you want to guarantee the smoothest results when migrating the User Profiles option, it's safest to have the user restart his or her computer before leaving work the night of (or weekend of) the migration. Otherwise, the remote agent may report that the user is still logged on. (This is a known issue with ADMT.) Quite a few users keep background processes running, such as mail and meeting software, so this is always the safest option.

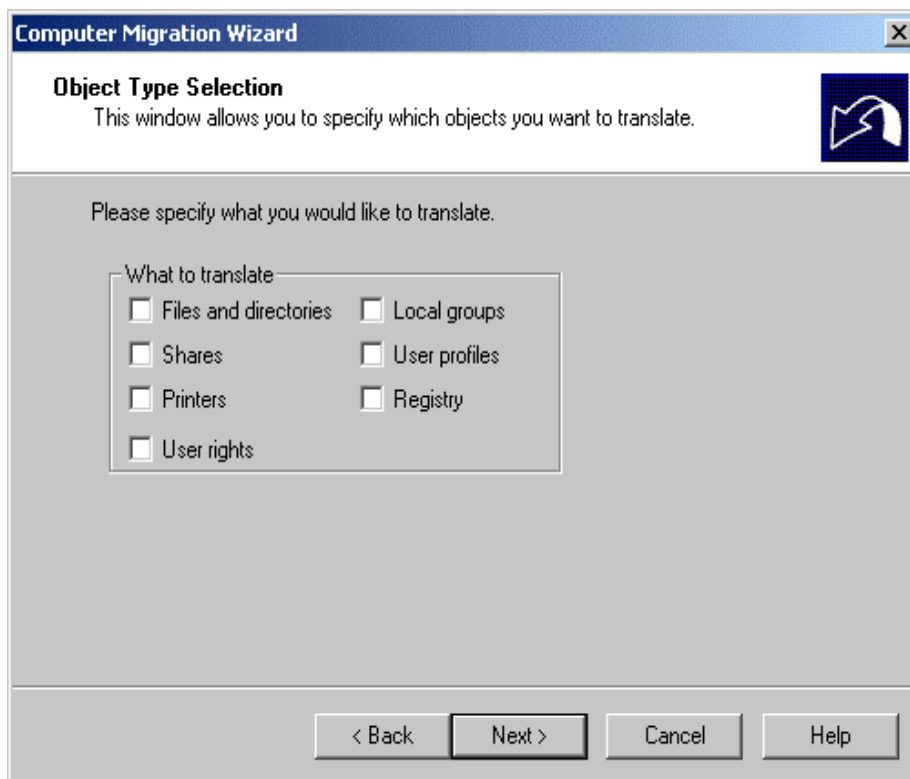


Figure 4.5: The objects that you can select in the Computer Migration Wizard.

When you migrate computer accounts from NT domains, ADMT doesn't migrate computer descriptions. This is because the Computer Description field is actually stored on the local computer and not in the NT-domain SAM database. If the source domain is Win2K, ADMT migrates computer descriptions. And also, do you have any computer names ending with the \$ character? If so, the Computer Migration Wizard creates the target computer account, but it's in a disabled state, an error is logged, and the computer's domain affiliation remains unchanged.

Finally, you can view information on the success or failure of the Computer Migration Wizard using the Event Viewer application log and security log on both the source and the target computers. These logs also contain information on the agent that is dispatched as part of the

migration. As with most applications, events are logged that need the original application installed to interpret the event ID, so the easiest way to read event log entries is on the computer on which ADMT is installed and remotely open the event logs on the migrated computer. Additional information logged to the Migration.log and Dispatch.log files can assist in case you need to troubleshoot the computer migration.

The Trust Migration Wizard

The Trust Migration Wizard is fairly straightforward. I mentioned earlier that you should use it only to create new trusts, not to verify existing trusts. The reason is that if a domain is listed as a trusted domain on both the source and the target domains, the wizard won't allow you to create a trust, even if that trust is broken. Also, if you use the wizard to create a trust from the target domain to an NT domain that trusts the target domain, the operation will fail, even though the wizard states that the trust was successfully created. You must manually create the trust. The migration also works only if the domain to be trusted is a Win2K domain.

Exchange Directory Translation

ADMT can also change security entries for Exchange objects, including mailboxes, distribution lists, custom recipients, organizations, sites, and containers. You can maintain access to Exchange throughout the migration by adding the newly migrated Win2K account to an object. Two requirements for doing so are:

- On the computer where you're running ADMT, install the Exchange Administrator console and connect to an Exchange 5.5 server
- You must be an administrator with the Permissions Admin role in the Exchange site for the Exchange server that you're connected to.

Active Directory Account Cleanup Wizard

The Active Directory Account Cleanup Wizard (ADACW) allows you to merge duplicate accounts that are created when multiple domains are migrated or upgraded to AD. The most likely reason that duplicate accounts occurs when the original Win2K account was created using ADC, and the NT account name doesn't match the alias in Exchange 5.5. You run the wizard from the Microsoft Exchange program group on the Start menu. It will identify duplicate accounts, based on matching SIDs, and merge the accounts that you select.

Migration Best Practices

Here are some approaches and techniques that you can consider as migration best practices to ensure a smooth migration.

Multi-Phase Methodology

Migration is best carried out using a multi-phase methodology, as discussed in Chapter 2 and illustrated in Figure 4.6 below. During the first four phases, the success of any one depends on the quality of work done in the previous phase(s). At any point in this process, you need to have

a migration plan in place based on the information gathered during the Define phase. The first four phases aren't carried out in isolation, however; rather, you'll continue asking questions and gathering information during each one that can affect your migration design. This is shown by the bottom arrows in the figure.

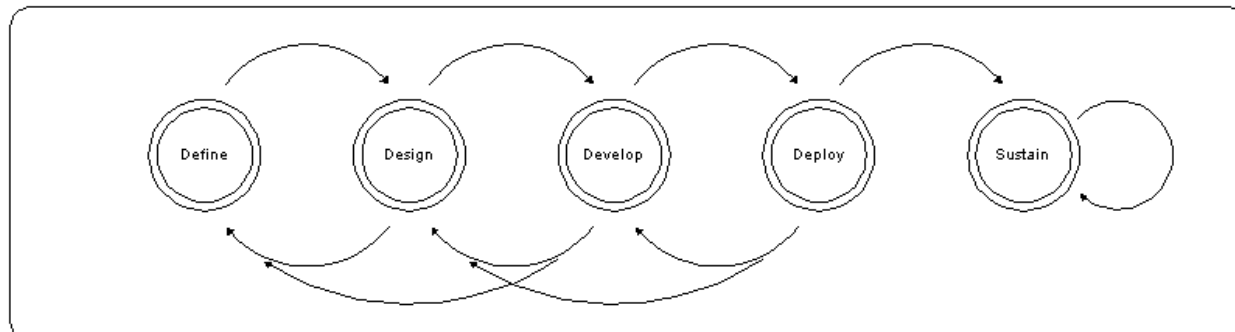


Figure 4.6: Multi-phase methodology diagram.

And the million-dollar question is: What are you going to learn from the migration experience that you'll wish you'd known from the start? If you know the answer to that one, you'll avoid some costly mistakes. This is where the lab environment pays for itself. The more you can learn in the test phase, the more money you'll save in deployment. Grab a backup tape from the domain controllers in each of your domains, restore to some lab servers (this will also help validate your recovery process), and run through the full set of procedures for the different migration types outlined earlier in this chapter. Then you can work out the gotchas that I mentioned.

Reviewing Naming Standards

Yawn! I know that reviewing corporate naming conventions is boring, but now is a good time to do it and establish a policy on how you'll deal with duplicate names. If you're merging multiple domains, be prepared for account- and even group-naming conflicts. Take a look at how ADMT deals with collisions (by adding a prefix or suffix, as shown in Figure 4.7) and determine which works best for you.

For example, your NT domains may have been limited geographically, so you may have a Sales group in the West domain as well as in the East domain. But now you must think on a larger scale, with a more integrated directory, and perhaps establish a naming convention that includes the geographic region as part of a group name. In this case, the two Sales groups don't have to fight it out over which one keeps their name.

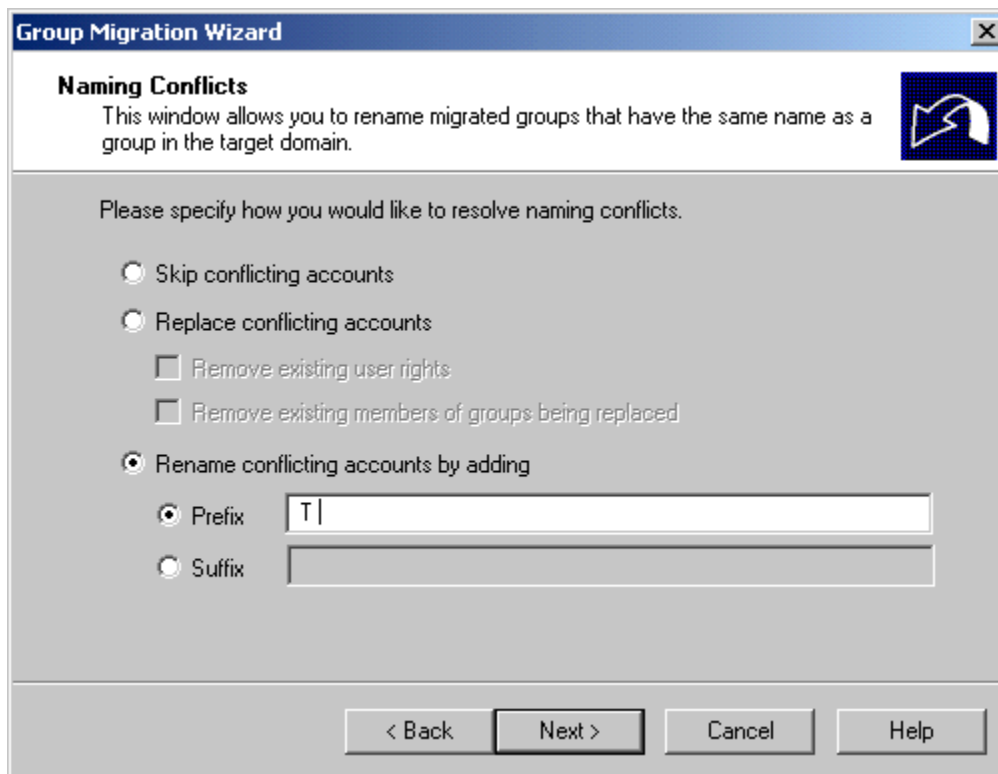


Figure 4.7: Renaming conflicting accounts when you migrate groups.

Setting Up Expectations

Key to this phase of migration is setting up people’s expectations about the process and outcome. This and the following chapters give you the information you need to communicate to your end users what type of migration process will be followed and what the impact will be. One of the third-party migration tools is marketed as “zero-impact,” but you know from what you’ve read so far that the impact will be greater than zero and should be a positive experience.

Validating Results

Throughout this chapter, I’ve given you checkpoints where you need to validate that users can access resources or where to look for information that is logged. Errors are usually logged, but you’ll get into the habit of reviewing log files as well. To explain this further, if you’re using ADMT to migrate with `sidHistory`, look for this entry in the log file:

```
<Time/Date Stamp>- SID for AccountName added to the SID History  
of AccountName
```

And if you can’t validate the results, it may be time to think about recovery.

Setting Up a Recovery Plan

Let me add this additional information to what I’ve already stated in “Having a Validated Recovery Plan” earlier in this chapter.

Rollback techniques—No matter what your migration approach, it's valuable to retain the old NT account until you're sure that there are no more unexpected problems. This is one advantage offered by inter-forest cloning tools, most notably the full-blown third-party tools as opposed to the Win2K Resource Kit utilities.

Phased migration approach—This allows users to continue using existing accounts and resources while you perform your magic in the background. The ultimate goal is complete transparency, where users aren't aware that changes are being made until they see the benefits and improvements.

Parallel approach—Users are able to use old and new accounts depending on the application or situation. This approach allows you to test new applications and make reconfiguration changes while the pilot (test) users go back to work in the old production domain.

Implementing Change Control

As with any organizational directory or network services, change control is essential to avoid exposing essential systems to risk of corruption or outages. The same is true of AD—the AD schema will need to be protected under a process of change control.

☞ When you upgrade to Exchange 2000, the AD schema will undergo several extensions (adding attributes or properties to existing objects). Installing ADC will extend the schema, as will installing Exchange 2000. I recommend that you not only do the extensions in this order but also run Exchange Setup with the /ForestPrep switch well before Exchange is installed. ForestPrep extends the AD schema to add the Exchange 2000 mailbox properties. Running ForestPrep in advance allows replication to complete and be verified across all domain controllers before installing Exchange 2000.

RID Pool Master Role


When migrating accounts among domains in the same forest, migration tools must communicate directly with the Relative ID (RID) pool master in the target domain. The reason for this is that the RID FSMO maintains the sequential list of security IDs to hand out. When you migrate large numbers of users and groups, you can improve performance by running the migration tools directly on the RID master or at least in the same high-speed network segment. Usually the RID master is the first domain controller installed in the domain unless someone has changed it. You can find the RID master by using the AD Users and Computers MMC snap-in or Ntdsutil.exe.

Playing Well with Others

This is just a playful reminder that in this phase, you're building the Win2K AD infrastructure with the intent to migrate to (or upgrade to) Exchange 2000, so you need to be aware of Exchange 2000 issues and needs. Here's an example of keeping Exchange 2000 in mind: When a new user is created in AD, the Full Name field is always generated in First, Last format. Next, this field sets the Display Name field so you end up with a global address list in First, Last format.


If this isn't the way your organization likes it, you need to use the ADSI Edit utility to modify AD to display in Last, First format. You can do this for global display of contacts as well as mailbox-enabled users. But you, as a Win2K administrator, will also benefit because ADSI Edit

also changes the Full Name field (that is, the cn field) so that users appear in the same format in the Users and Computers MMC snap-in.

 For information on using ADSI Edit, see Microsoft Knowledge Base article [Q277717](http://support.microsoft.com/kb/q277717). For procedures on how to change display names using Active Directory Service Interfaces (ADSI) scripting, see [Q250455](http://support.microsoft.com/kb/q250455).


Security Considerations

Because you've introduced a new OS into your network environment, you must stay up to date with security announcements and patches or hotfixes released by Microsoft. You'll experience a definite learning curve as you get used to the security tools in Win2K, and this would be an ideal time to hire an outside network security specialist to perform a security audit.

 I've seen many companies throw money away on security audits by either hiring under-qualified consultants or not adequately preparing the security experts. To protect against this, have your internal security team perform their own audit and present a summary to the experts. This will allow your company to avoid the high cost of consultants telling you what you already know: that you must increase your password length and rotation policy!

An immediate issue with inter-forest migrations is that they require you to use cloning techniques to preserve the old account access (using the SID) in the new forest (using sIDHistory). If customers are extremely concerned about security—for example, in an environment where the system administrators manage network resources but must have absolutely no access to organizational information that may be top secret—sIDHistory presents a slight security risk.

Until the source account is removed, sIDHistory allows two accounts to gain access to resources using the same SID, and an administrator could take advantage of this situation by cloning the SID to a new account, resetting the password on the account, then using it to gain access to confidential or sensitive information. The solution is to either disallow cloning tools or closely monitor their usage and the usage of the resulting accounts.

 You can get a jump-start on your security audit using checklists and tools from this Microsoft site: <http://www.microsoft.com/technet/security/tools.asp>.

Subscribe to security announcements and patches or hotfixes released by Microsoft from: <http://www.microsoft.com/technet/security/notify.asp>.

Password Policies

This chapter has made several references to problems with migrating accounts and running into problems as a result of domain-password policies. Some administrators choose to turn off strong password policies during migration to avoid such problems. However, there is a right way and a wrong way to do this. The wrong way is to clear the Minimum Password Length Policy check box in the Active Directory Users and Computers console; when users try to log on, their passwords aren't accepted! The right way is to set the password policy to zero, apply the change,

then clear the Minimum Password Length Policy check box. If you're still having trouble allowing users to change their passwords, you may have to resort to allowing the Change Password permission for the Everyone group.

Looking to the Future

As you finish your migration to Win2K, the next version of the OS will be nearing release or be shipping. There's nothing wrong with that. My advice is to take your time and get Win2K right. It's a major update to NT, especially in how it provides directory and network services. But it's ironic that only when the new version comes out will you fully see the limitations of the previous version. You know the story; you find out that the previous product had certain limitations as the new product addresses them. Nevertheless, you must keep moving to provide your organization or company with technological competitive advantage. And from here, you'll migrate to Exchange 2000, a major leap in technology.

Summary

In this chapter, I looked at the many tools you can use to build your Win2K infrastructure, including moving user and computer accounts and groups to AD. The first set of tools is for gathering information and reporting to better prepare you and identify the problems that you may face. I stressed the importance of having a validated recovery plan in place and using a lab for verification.

Then I described the differences between doing your migration as an in-place upgrade or incrementally. I discussed the issues of migrating SIDs across domains and forests as well as the tools that can help you re-ACL the resources involved. Next, I walked you through using the ADMT wizards for actually performing the migrations, showing you along the way where it may or may not be the right tool to use. Finally, I offered some general migration best practices to help you no matter which migration path you choose.

In the next chapter, I'll deal with some of the more painful issues of migration: the ongoing care and feeding of your new environment, which is related to the sustaining component of your migration process. Once the task of migration has been undertaken and perceived to be complete, many steps can be forgotten.

Copyright statement

This site contains materials created, developed, or commissioned by Realtimepublishers.com, Inc. and is protected by international copyright and trademark laws. No material (including but not limited to the text, images, audio, and/or video) may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.