

Chapter 5: Managing Post-Migration Tasks in Windows 2000

Now that you're at the stage where you have enough information and you've actually performed a migration, the question is: What now?

The project outline provided in Chapter 2 (see "Determining a Planning Methodology") included the concept of ongoing support and maintenance. This is where it comes into play. Once you've completed the actual migration, you still need to do a lot of work to ensure that your system is running smoothly and to make the most of the new capabilities you've introduced.

The first step is to ensure that you understand what your business expects of a Service Level Agreement (SLA). There is a recent trend to talk about business goals in terms of "the number of nines uptime." For example, 99.999% uptime, known as the "five nines," equates to less than five minutes of downtime per year. When you encounter this type of SLA, you need to determine what exactly you're measuring. The answers to this question provide the basis for your SLA, which may include specific levels to do with particular aspects of the service, such as Name Services, Directory Services, accessibility, and more.

The reality is that most applications can deal with four nines, or 99.99% uptime, which equates to around an hour of downtime per year. Many of you familiar with Windows platforms will probably laugh a little, given the number of times you tend to be forced to restart a computer to install new software or implement service packs. However, most measurements used to compare against an SLA regularly exclude scheduled maintenance and upgrades.

A common approach to ensuring that Information Technology (IT) departments don't suffer from unanticipated outages, and one that I recommend for an organization of any size, is to formally schedule a regular maintenance window when systems will be unavailable for regular access. This should also form part of any SLA that you have with the business.

Having a maintenance window doesn't mean that you have to use any, or all, of the allocated time, but it does ensure that you have a fair opportunity to maintain your environment. Many organizations already do this, and if you don't currently schedule a maintenance window, consider it now. The big advantage of scheduling downtime during off-hours is that you reduce the risks of unscheduled downtime occurring during more regular production hours. You may need to give the appropriate business representatives advance notice, such as by e-mail or voice-mail, so that they can ensure that there is no conflict with important business activities. If an organization uses an intranet (more and more companies are), you can use the corporate intranet to advise business users of these times.

Cleaning Up after Migration

Once you've performed your migration, you need to deal with the cleanup aspects of the job, such as retiring any old accounts, domains, and servers. This effort is often overlooked and then likely to be squeezed out by other, more pressing priorities. In this chapter, I'll clarify and simplify the process so that you can benefit from regaining those network resources.

Reviewing the Documentation

Throughout the migration process, you'll have referred to your documentation: the project plan, the audit information, network diagrams, and so on.

If you haven't been reviewing and updating these documents (online, printed, or otherwise), now is the time to do so, based on the migration. This will be especially useful, if not essential, for planning purposes and to provide a decent level of maintenance for your new environment.

The first step is to make a list of what documentation is available, then what is required (or vice versa—if you know what is already available, you have a good starting point). Using these two lists, you can determine the gap, then create a plan to bridge that gap. You also need to schedule each document for ongoing review. Ongoing review is often left to chance, but having up-to-date documentation is crucial. During a disaster-recovery scenario, for example, it can save your business.

What documents do you need? Here is a suggested list of documents that you must own, or identify an owner for, in your organization to successfully use any network environment, including Windows 2000 (Win2K). There may be other documents that you normally use, or your organization may use different names for them. In any case, these are the core documents that you need to keep updated as you clean up after migration.

- Network diagrams
- Domain structure
- Security policies (both Windows-specific and general corporate policies)
- Hardware inventory and configuration
- Software inventory and configuration
- Disaster-recovery plan (based on your SLA, approved by management, and formally and regularly tested)
- Ongoing maintenance schedule (for these documents and installation in general)
- Emergency contact list and processes, including partners (such as telecommunications companies and support and maintenance groups).

Defining the Tasks

To define the cleanup process, you need to focus on many aspects of your new environment. In small installations, this won't be a major issue, but in larger ones, depending on the number of users and/or servers you migrate, you'll likely find that a large amount of baggage came over during migration. I list the high-priority focus points below. Be forewarned that you probably won't be able to undertake many of them with the base tools that Microsoft provides, so you'll need to use third-party tools, or the effort will likely be overwhelming.

- Eliminate historical Windows NT domains no longer considered important enough to keep
- Eliminate historical NT accounts that were migrated but that either are no longer required or pose a security risk

- Remove legacy NT Access Control Entries (ACEs)
- Remove unresolved security identifiers (SIDs) in any resource discretionary access control list (DACL) (specifically, review the sidHistory attribute for all user and group objects migrated to the new domains and identify any broken trusts that still exist)
- Retire legacy servers
- Review any extraneous Windows Internet Name Service (WINS) or Domain Name System (DNS) entries.

On the system- and account-management side, you'll also need to consider:

- Assigning delegated administration
- Reviewing and validating management breakdown among security, networking, Windows, and Exchange administrators (and anyone else who has a vested or intrinsic interest).

Figure 5.1 shows how you can move (also called “prune and graft”) one object, such as user or computer objects, from one Organizational Unit (OU) to another in Active Directory (AD). There is no simple drag-and-drop mechanism, and worse still, no way to move groups. If you want to make bulk moves, you can script the process using tools like the LDIF Directory Synchronization Bulk Import/Export tool (LDIFDE) or MoveTree.

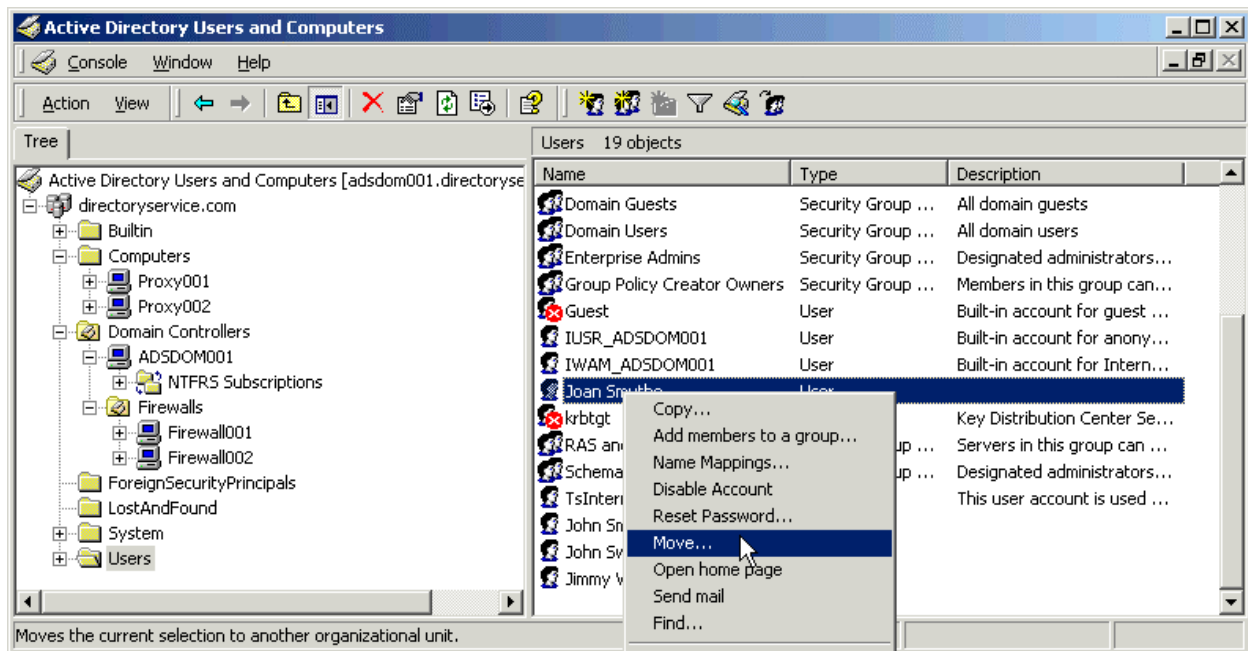


Figure 5.1: Moving an object around AD.

Restructuring Domains

As I said earlier, Win2K AD domains are much more scalable than NT 4.0 domains. Chapter 3 discussed AD design and how you can either consolidate your domains as you migrate or do it afterwards. Here are the key areas to consider when you review restructuring your domains:

- Maintaining legacy NT installations and applications
- Delegating administration
- Reviewing security.

I'll discuss the first two areas now and review security later in this chapter.

Maintaining Legacy NT Installations and Applications

One of the options you have is to eliminate any extraneous resource domains that you can now manage more effectively using OUs and to carry out appropriate delegated administration using AD permissions and Group Policy. To retire resource domains, you need to begin to move the resource-domain resources into OUs in your new AD domains.

To determine whether to eliminate or consolidate resource domains, consider these criteria.

- **Application development**—One common reason that resource domains exist is that they may be used to test new code and even changes to the AD schema. These resource domains aren't good candidates for consolidation because developers need to try new applications, services, and their own code before anyone else is affected without any level of quality assurance.
- **Delegated administration concerns**—Another common reason that resource domains exist. In Win2K, you no longer need to create separate domains to manage granular management controls. If this is your primary concern, give the appropriate administrators control over an OU that represents their specific groups of users and computers, one that was previously their resource domain.
- **Password policy**—If a specific group maintains a separate and distinct password policy from the rest of the organization, it might make consolidation ineffective. A common example is a compliance group, found in the finance industry, amongst others. Nevertheless, NT domains can be consolidated into the AD forest.

In Chapter 2, I suggested that you audit for and identify any applications in place on the network. (See "Taking Inventory of the Network.") At that time, you'll have identified applications that required upgrades to support Win2K and those for which there was no upgrade path. In cases where you need to maintain existing domains, you have a couple of options.

- You can simply create a tree with transitive trusts, or create the appropriate trusts among existing trees, so that information can be shared but managed separately as required. This will require you to maintain your network in mixed mode for some time.
- You can use one of the available third-party management tools, such as those from NetIQ Corporation and Quest Software (formerly FastLane Technologies), which allow you to manage accounts and policies across NT and Win2K environments. While this could turn into an expensive proposition, it may solve the problem you face for less than it would cost to migrate the legacy application or service.



A key reason for migrating to Win2K is the functionality and extensibility AD provides and the interrelated components at the core of Win2K. Keep in mind that running in mixed mode means more work for you and also limits your ability to offer your business the optimum functionality of Win2K. Until you run a pure Win2K environment, you won't achieve the full benefits of Win2K.

Of course, if you're migrating, you'll need to run in mixed mode until you can conclude a full migration. Many limiting factors force you to do so, including non-compliant applications, resource constraints, budget deficiencies, and more.

Reviewing Your Design for Delegated Administration

In Chapter 3, I took you through planning your AD tree structure. (See "Planning the AD Namespace.") You'll have put a lot of thought into this, and now that the migration has taken place, you'll be able to determine if it actually delivered on the requirements that you determined in your planning. One item that you should review is your administration model. Compare the following questions with your original assumptions:

- Is your AD model so secure and simple that administrators believe they have enough control to manage their user population?
- Did the migration provide the projected benefits of efficiency and cost-savings from delegated administration?

If the answer to either of these questions is no, it's time to go over your design for delegated administration and determine whether it needs to be changed. Have another look at the 4DS project process described in Chapter 2 (see Figure 2.1). It includes continuous reviews as well as the loop effect, both of which allow time to go back over steps in continuously improving cycles. Your OU design may not be expansive or expressive enough to support expectations such as administrative or policy-management boundaries.

Of course, the benefit of Win2K is that you can move objects around AD with relative ease, enjoying the full benefits of generalized policies being applied to specific OUs, providing delegated administration capabilities using OUs as boundaries and containers. AD also allows more granularity at the object level when required, but this should be used sparingly because it becomes hard to track and could affect the performance of the operating system (OS) in processing excessive policies. Certainly, however, these capabilities are greater than were ever offered in NT environments.

Using Third-Party Tools

Although Microsoft tools exist to help manage and maintain your new Win2K environment, you should also consider more comprehensive tools offered by third-party vendors. As I said earlier, the time you spend cleaning up using the tools available in the base Win2K installation, or even in the Microsoft resource kits, is potentially extensive.

If you used one or more third-party tools for your migration, you'll find that most of them offer inherent functionality to manage your new environment and, for additional cost, extended functionality. Many include advances in the concept of managing mixed-mode environments and can solve many issues, such as the potential conflicts between Win2K and NT policies. I'll

review a few of the more familiar third-party tools, but numerous other companies offer such products too.

Another consideration with many of these vendors is that they offer integrated tools whose management capabilities extend beyond the core Win2K environment. In most cases, Exchange 2000 (E2K) is also supported in some fashion, and beyond that, a lot of the Microsoft BackOffice applications are coming online.

From NetIQ Corporation

NetIQ Corporation recently announced the packaging of five of their migration tools under the banner of the “NetIQ Migration Suite”, which essentially provides a complete migration solution for a majority of corporate situations.

The following tools are available for purchase separately or as the complete migration suite:

- **Domain Migration Administrator:** Accelerated domain consolidation and migration from Windows NT to Windows 2000.
- **Server Consolidator:** Simplified file and print server consolidation, replacement and upgrades.
- **Exchange Migrator:** Allows you to move Exchange objects from one Exchange organization or site.
- **Migration Assessor:** Assess and report on your environment before, during, and after your migration.
- **NetIQ NetWare Migrator:** Accelerated migrations from Novell Netware to Windows NT and Windows 2000 environments.

Of importance to this discussion are the Domain Migration Administrator and Exchange Migrator.

Domain Migration Administrator accelerates domain consolidation and migration to Win2K. Its automation features enable you to migrate user accounts and their passwords, groups, trusts, member servers, workstations, user rights, and security settings between NT and Win2K domains – all while preserving access to existing resources and without disrupting end users.

By using additional utilities, Domain Migration Administrator can help with ongoing management. In general operations mode, ongoing control is managed using the Directory and Resource Administrator which offers file security, reporting, and service account administration.

With File and Storage Administrator you can delegate file, folder, share, and quota management across both NT and Win2K domains. It also lets you implement security policies for files, such as locating MPEG Audio Layer-3 (MP3) files and taking a predefined action such as deleting, moving, or setting the Access Control List (ACL) to deny access to those files.

Exchange Migrator allows you to support Exchange 5.5 to Exchange 2000 migration, as well as Exchange 5.5 to Exchange 5.5 migration in inter-site and inter-organization scenarios.

From BindView Corporation

BindView Corporation's bv tools offer a lot of functionality to assist with the migration process, but they also help you maintain the Win2K environment using a project-based interface. For example, bv-Admin, one of the tools in the tool set, has a primary goal of advancing the ability of administrators to set up delegated administration in NT domains, allowing those undertaking the migration to select objects from multiple domain sources to migrate on the fly without having to consolidate domains beforehand. While not as useful as the NetIQ products, BindView's offering is considered more advanced in the general ongoing administration space than the standard Microsoft tools.

From Quest Software

Quest Software (formerly FastLane Technologies) offers another large set of tools for handling migration. In fact, FastLane Migrator (formerly DM/Manager) and FastLane Administrator are all useful during migration and can play as large a part as you want, especially if you don't migrate from NT 4.0 in a hurry. Now that you face the ongoing management of the domain, Quest offers the FastLane Active Roles solution. Essentially, it abstracts groupings and settings into logical bundles that you can then apply to other groups of users. This product is more advanced than that offered by the basic User Administration from Microsoft. It will likely help large companies but could be overkill for companies with fewer than 500 users.

Maintaining Active Directory

Because AD is the core service for a robust Win2K network, you need to ensure that your AD is safe and healthy. You do this by maintaining and monitoring it regularly. Administrator utilities allow you to monitor the health of the AD servers, state of replication, and performance details.

Managing and Modifying the Schema

This section discusses the ability and potential need to modify the AD schema. It also talks about managing the schema from the point of view of:

- Deciding who will be assigned to manage it
- Managing changes to it
- Using the Global Catalog.

Ownership of the Schema

You need to decide early on who owns (is responsible for managing) the schema or, perhaps more specifically, protecting the directory schema. This is essential for several reasons.

- Adverse situations may arise because of an unplanned or malicious schema change—just as with any other change to your network
- Making multiple changes to the schema can create potential conflicts
- Applying indexes incorrectly can have an adverse impact on replication.

Managing Changes

Some applications will be delivered with their own schema changes. You should carefully scrutinize them and evaluate them against your test domains. The information you collect should then be evaluated by those assigned to manage the schema.

Administrators can update AD with schema extensions, whereby applications can use custom directory objects. Administrators can also manage schema extensions using the new Windows 2000 AD administration tools. This also allows users and applications to use a standard and effective mechanism to publish information to each other.

You may intend to deploy an internal self-service application that allows users to update their own information and request services from the organization. If so, you might need to create a custom object class that includes information specific to your business and add attributes for building number, floor number, desk number, health plan and related information, and so on.

Managing AD can be a very political situation as well as a technical challenge, so you need to address this early on in your migration effort. You may also want to identify high-level support for this activity, as well as external consultants who've handled this activity before. As much as you can deal with any potential political issues in your organization, you must also deal with those who want to use applications that use the capabilities inherent in AD.

AD supports many naming, query, registration, and resolution needs. This is how most of the Win2K OS is structured, taking its naming conventions from the structure that was created when you first defined the namespace for your Win2K installation. Because this resource is now also available to other applications, you need to anticipate a time when you'll extend the AD schema.

Chapter 3 discussed how to structure your domains and OUs and how to represent this structure in the AD domain. In OUs, you can create, manage, and look up computers and users. In fact, AD already defines a wide variety of classes beyond these, providing standard object classes for Domain, Group, Machine, Volume, and PrintQueue.

Beyond these classes, there are sets of rules, policies, Component Object Model (COM) component configuration, and networking objects that allow the OS and any application with the proper setup and access to maximize its understanding and use of the network environment based on the common understanding of the model in AD. For example, conferencing over the network allows users to locate others, identifies users across the network, requests a call wherever they're logged in, then using the information in the directory, determines what type of communication is optimal for the devices used in the conference.

Using the Global Catalog

Another thing that you need to consider in managing the schema is the fact that a copy of every object is stored in AD as part of the Global Catalog (GC). The GC is a service that manages and maintains information on all objects in any domains in a forest. (This is beyond a single domain tree.) The GC acts as a high-speed index of all objects that may be distributed throughout the tree, allowing applications and users to quickly find objects, even if they're not in a local copy of the directory.

The word *catalog* is appropriate because it allows you to do a quick search on key terms, or in this case attributes, then provides a pointer to where the more complete information is stored. It acts much like the catalog service you find in your local library.

One example of how the GC works occurs when network services need to locate a printer object. Let's say that you work in a large company with many offices. You happen to be in a new office for the day, and you need to urgently print a PostScript document. Searching AD identifies that the Marketing Department has the only PostScript printer in the building. You didn't have to ask around the building, and in no time, you've loaded the printer driver and are printing away.

As an example of an application that makes schema modifications and uses the GC in a way that is relevant and recognizable for most of you, consider installing E2K. It adds messaging-specific attributes and object classes and now uses the GC as an extension of the Global Address List (GAL) to look up mail recipients across domains.

Pruning and Grafting

I have to offer the opinion that this release of AD, and its related management tools, leaves a little to be desired in terms of ease of use for pruning and grafting. There is currently no drag-and-drop functionality in the Microsoft Management Console (MMC) environment, and detractors of the system have long raised this as an issue. For example, let's say you're splitting a group of 5,000 users into two departments. The existing Win2K tool doesn't support bulk moves, so this would be a laborious and time-consuming task. If you find that during migration, you're doing a lot of pruning and grafting as you move objects around AD to ensure that they reside in the right place, the third-party utilities I discuss throughout the chapter can help you.

That said, however, you can move single objects around AD quite easily using the Active Directory Users and Computers MMC snap-in. This tool allows you to select an object, right-click it, then choose Move Object from the shortcut menu. You can then move the object anywhere in the directory tree. An example occurs when a user moves from a Sales role to Engineering. (Laugh as you may, it happens.) If you have users in OUs that represent departments, you can easily want to move this user from the Sales OU to the Engineering OU.

Maintaining Windows 2000


In this section, I'll review maintaining several vital aspects of your Win2K environment. Some of these will be different from the NT environments you may be familiar with. Specifically, I'll focus on:

- Backing up and recovering Win2K
- Recovering in an emergency—including using the Emergency Repair Disk (ERD) and the Recovery Console
- Preparing for disaster
- Applying patches, updates, and utilities.

Backing Up and Recovering

Chapter 4 discussed the importance of developing a backup and recovery plan before you migrate from NT 4.0. When your Win2K environment is running normally, you also need to consider two aspects of this plan, probably similar to what you had with your NT infrastructure.

The first aspect has to do with general data and application service; while this is important, I don't discuss it in this book. What I will discuss is the second aspect: backing up and recovering your AD services.

 Microsoft provides detailed documents on the backup and recovery processes. Much of this information applies even if you use a third-party backup utility and not the one included with Win2K. See:

“Windows 2000 Server Disaster Recovery Guidelines” at
www.microsoft.com/windows2000/docs/recovery.doc

“Active Directory Disaster Recovery” at
www.microsoft.com/windows2000/docs/disaster.doc

Backing Up the System

As I discussed in Chapter 2, you need to review your existing backup tool for compatibility with Win2K, and this includes any agents that you may have running. Now is a good time to check this, especially if you plan to migrate soon to E2K.

A good Win2K backup includes the complete *System State*—which includes AD—the complete system drive, and the SYSVOL folder (if it's not located on the system drive). To completely back up all of these components, you need to log in to the system as a member of either the Backup Operators group or the Administrators group. A good backup also takes into consideration how often you make backups and the type of backup you make. For example, if you make backups only once a week, you can potentially lose up to seven days' worth of data. For most organizations, this is a significant amount of data to lose.


The System State of a domain controller includes several components that are essential to running the system, and they fully depend on each other to work cohesively. If you use the Win2K Backup utility, you must back up these components together and restore them together to ensure good performance. (However, NetBackup from VERITAS Software allows you to perform these tasks separately.) These components are listed in Table 5.1.

This Component	Does This
System startup files	Ensure that Win2K starts successfully.
System Registry	The contents of the Registry are automatically included in a System State backup. In addition, when you create an ERD, a copy of the Registry is placed in the %SystemRoot%\Repair\Regback folder, allowing you to restore the Registry without completely restoring the System State.
Class registration database of COM+	COM is a binary standard for writing component software in a distributed systems environment. The Component Services class registration database is backed up and restored with the System State data.
SYSVOL	The system volume provides a default AD location for files that must be shared for common access throughout a domain. The SYSVOL folder on a

This Component	Does This
	<p>domain controller contains the following:</p> <ul style="list-style-type: none">• NETLOGON shares (usually host logon scripts and policy objects for non-Win2K-based network clients)• File system junctions• User logon scripts for Windows 2000 Professional-based clients and clients running Windows 95, Windows 98, or NT 4.0• Win2K Group Policy files• File Replication service (FRS) staging directories and files that must be available and synchronized among domain controllers.

Active Directory	Includes: <ul style="list-style-type: none"> • Ntds.dit—the AD database • Edb.chk—the checkpoint file • Edb*.log—the transaction logs, each of which are 10 Megabytes (MB) in size • Res1.log and Res2.log—reserved transaction logs.
	In addition, if you're running AD-integrated DNS, the zone data is backed up as part of the AD database.

Table 5.1: The components that are included when you back up the System State.

 You can restore a backup from a specific domain controller only to that domain controller. This very important consideration will affect your backup strategy. The minimum, and most essential, domain controllers that you need to back up are all of the operations master role holders, as described in Chapter 2 (see “Operations Masters”), and the first domain controller in the root domain. This allows you to recover other domain controllers by reinstalling, replicating, and, at worst, recovering the data.

The Win2K Backup utility supports several types of backup, including:

- Normal
- Copy
- Incremental
- Differential.

The only way to back up the System State, including AD and related information, is to perform a normal backup, also known as the full method. A normal backup backs up the entire System State while the domain controller is online. In addition, it marks each file as having been backed up, and this clears the archive attribute of the file. Any Win2K-aware backup utility can back up the System State, and Figure 5.2 shows the Win2K Backup utility ready to do so.

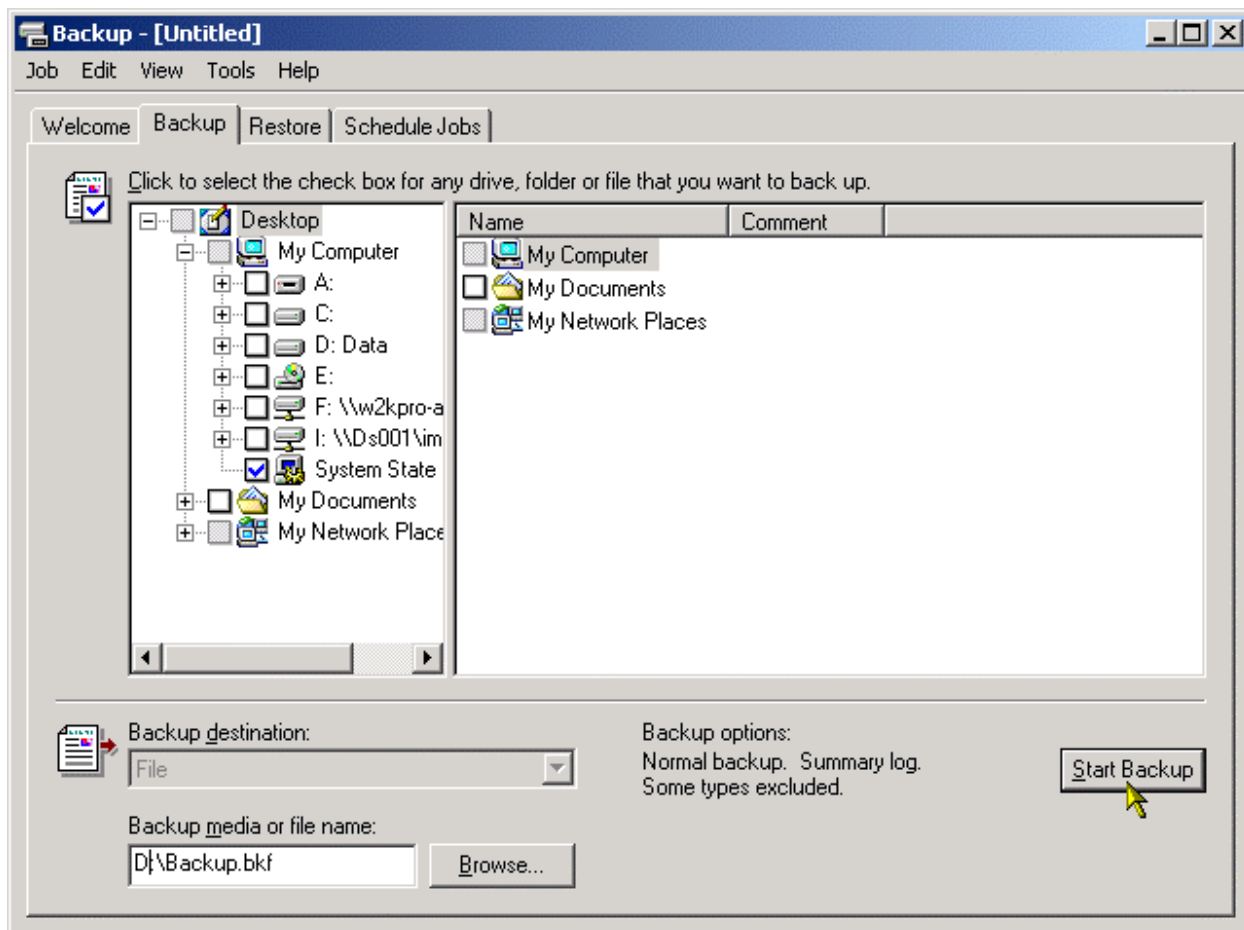



Figure 5.2: Using the Win2K Backup utility to back up the System State.

Backup Tools

It's important that you use a good backup tool. While Microsoft's own Backup utility is quite effective for the base OS and, to a degree, E2K, more advanced tools offer agents that work with other applications such as Exchange and SQL Server. These tools include ARCserve 2000 from Computer Associates, Backup Exec and NetBackup from VERITAS Software, NetWorker from Legato Systems, UltraBac from ULTRABAC.COM (BEI Corporation), and many others.

 As defined by Microsoft, the most important consideration with backups and “tombstones” is that the domain controller be restored before the tombstone expires and that inbound replication to the restored domain controller from a domain controller containing the tombstone be completed before the tombstone expires.

When AD recognizes that data being restored is older than the “tombstone lifetime,” it disallows the restore. As a result, the useful life of a backup is equivalent to the tombstone lifetime setting for the enterprise.

Recovering the System

If you need to recover a Win2K system, you can use the Setup utility in a special Repair mode. You can access the recovery option using the Windows 2000 installation process (on CD-ROM or floppy disk) or the Recovery Console. The recovery option can help resolve general startup problems. For more specific problems, use the Recovery Console. (See “Using the Recovery Console” later in this chapter.)

Recovering in an Emergency

There are two primary methods for recovering a Win2K domain controller:

- Reinstalling
- Restoring from backup.

 For a complete discussion of these options and the associated process, review the Microsoft recovery paper “Active Directory Disaster Recovery” at www.microsoft.com/windows2000/docs/disaster.doc.

In addition, you need to know how to repair startup failures caused by invalid Registry data.

The system Registry is the core of a Win2K server. The Registry has been acknowledged as one of the most common places for a system to fail. For some reason, it can become corrupt—either physically, from a hardware failure, or logically, from a software error. Because it’s difficult to tell what the cause of the damage is, it may not be a problem with the Registry at all. However, if you suspect a Registry-related problem, the first line of defense is to restore a previous known-good Registry configuration. You can do this using one of three methods:

- **Last Known Good Configuration Boot Option**—Press F8 at the Win2K Boot Loader menu, then choose this option from the Advanced Options menu. It allows you to restore a previous system configuration and can be one of the quickest and easiest solutions to a startup blue screen—if it works. If the Registry is corrupt, it will fail because it relies on the Registry itself to function. Thus, many have found that this option isn’t very successful. (For more about this option, see “Using the Boot Loader Menu” later in this chapter.)
- **Emergency Repair Process Fast Mode**—Use the Fast Repair option in the Win2K Setup program’s Emergency Repair Process. However, as I mentioned earlier (see “Recovering the System”), the system itself determines which Registry files should be replaced and the source of those files (the %Systemroot%\Repair folder); there is no user intervention during this process.
- **Manually replacing Registry hive files**—Use known-good copies that you saved in an alternate location—for example, on a removable disk or in the %Systemroot%\Repair or %Systemroot%\Repair\Regback folder. (The latter is created by Win2K’s Backup utility during a System State backup, which I described earlier in “Backing Up the System.”)

Preparing for Disaster

If you've been a good administrator of your NT 4.0 systems, you've made a habit of updating each server's ERD regularly and, what's perhaps most important, before and after each system upgrade. This allowed you some level of comfort and probability of recovery should some disaster befall your system. As you look at Win2K, you'll note that the time-honored `rdisk.exe` tool no longer exists. This is because the process has changed significantly and because Microsoft has added a few tricks to the recovery process.

Using the Emergency Repair Disk

In a large NT 4.0 installation, you may have found that you couldn't create an ERD on a single floppy disk because the Registry files were too large. Because in Win2K they're even larger, it's impossible for any ERD to include the Registry. So Microsoft backs up essentially only the following files to the ERD:

- **Autoexec.nt**—A copy of the `%Systemroot%\System32\Autoexec.nt` file; it initializes the MS-DOS virtual DOS machine (VDM) environment, which runs MS-DOS and 16-bit Windows applications
- **Config.nt**—A copy of the `%Systemroot%\System32\Config.nt` file; it initializes the MS-DOS VDM environment, which runs MS-DOS and 16-bit Windows applications
- **Setup.log**—A log of files installed, along with checksum information, when you run Win2K Setup and choose the Emergency Repair Process option. This log verifies files against their original source copies on the Win2K installation source (for example, the Windows 2000 CD-ROM).

In addition, Microsoft relies on the rest of the system being backed up into the `%SystemRoot%` repair folder (such as `C:\winnt\repair`).

The intent is that when the OS starts up, even from an ERD, it should be able to initialize the startup environment, verify existing Win2K system files and the boot sector, then use the repair folder to restore corrupt Registry or system files. If the server should fail in any significant fashion—for example, if your system partition becomes corrupt or worse—this doesn't actually help you that much. So the obvious choice is to ensure that after you back up the System State, you also move the repair folder to a proper backup file or dated folder on a backup server.

To use the ERD, you need to start in recovery mode using the Setup floppies, the Windows 2000 Setup CD-ROM, or the Recovery Console boot option. For information on installing this option, see "Installing the Recovery Console to the Startup Options" later in this chapter.

You have two choices for recovery:

- **Manual Repair**—This mode (choose M from the Emergency Repair Process menu) gives you full manual control over the repair process. You can do one or more of the following: inspect/repair the startup environment (the files required to start Win2K), verify/repair the Win2K system files, and inspect/repair the Win2K boot sector. If any of these steps will replace the respective component(s), you're asked to confirm them.

The main issue with Manual Repair mode is that it doesn't provide an option to restore the Registry hive files; these could be important in some situations, such as where application-specific data has been written to them. For example, most Microsoft applications use the Registry to store local data, so consider backing up any Microsoft BackOffice application server.

- **Fast Repair**—This mode (choose F from the Emergency Repair Process menu) is essentially an automated “kitchen sink” repair mode. It verifies and replaces all of the system components, plus the system Registry files, if the system deems it necessary (for example, because of an error or discrepancy in the data). Unfortunately, because this process is fully automated, you can't control what does or doesn't get replaced, so it's best to use this option only occasionally.

Unlike Manual Repair mode, Fast Repair replaces the Registry hive files. However, because it's completely automated, it doesn't allow you to control which files are replaced. This is an issue, for example, if you want to select specific files to restore.

Note that the ERD isn't a boot disk. In fact, if you leave the ERD in your floppy drive and restart, you'll likely see a nasty message that NTLDR can't be found.


ERDisk

If you don't like the idea of using Win2K's Backup utility (the new tool for creating and updating ERDs) at each computer to manually update ERDs on all your systems, there are better solutions available. One product to consider is Aelita Software's ERDisk. It lets you create remote Win2K and NT ERDs across the network for multiple computers, and it also sports remote-recovery features. You can find more information on ERDisk at www.aelita.com.

Creating the Emergency Repair Disk

In essence, creating the ERD is still important in Win2K because it ensures that system files and Registry entries are backed up so that the Win2K Setup Repair process can locate the Win2K installation that you want to recover. Although Setup might normally be able to do this without the help of the ERD, there are some situations in which the installation cannot be found, such as when a boot sector is corrupted, so the ERD is still essential.

Creating an ERD is a relatively simple process. It uses the Win2K Backup utility.

-  A bug in the Win2K Backup utility prevents hard disk-based copies of the Registry files and the ERD floppy disk from being created if the %Systemroot%\Repair folder is missing or empty when you attempt to create the ERD. Therefore, if this folder is empty (that is, either because you deleted it or moved or deleted the files), you may need to restore it temporarily from a copy made on either that system or another system. This issue has not been resolved as of the release of Service Pack 2.

To create an ERD:

1. Insert a formatted, blank floppy disk labeled as your ERD as well as with the server name and creation date.
2. Select Start>Programs>Accessories>System Tools>Backup.

3. In the Backup utility, click Emergency Repair Disk, as shown in Figure 5.3 (or choose Tools>Create ERD).

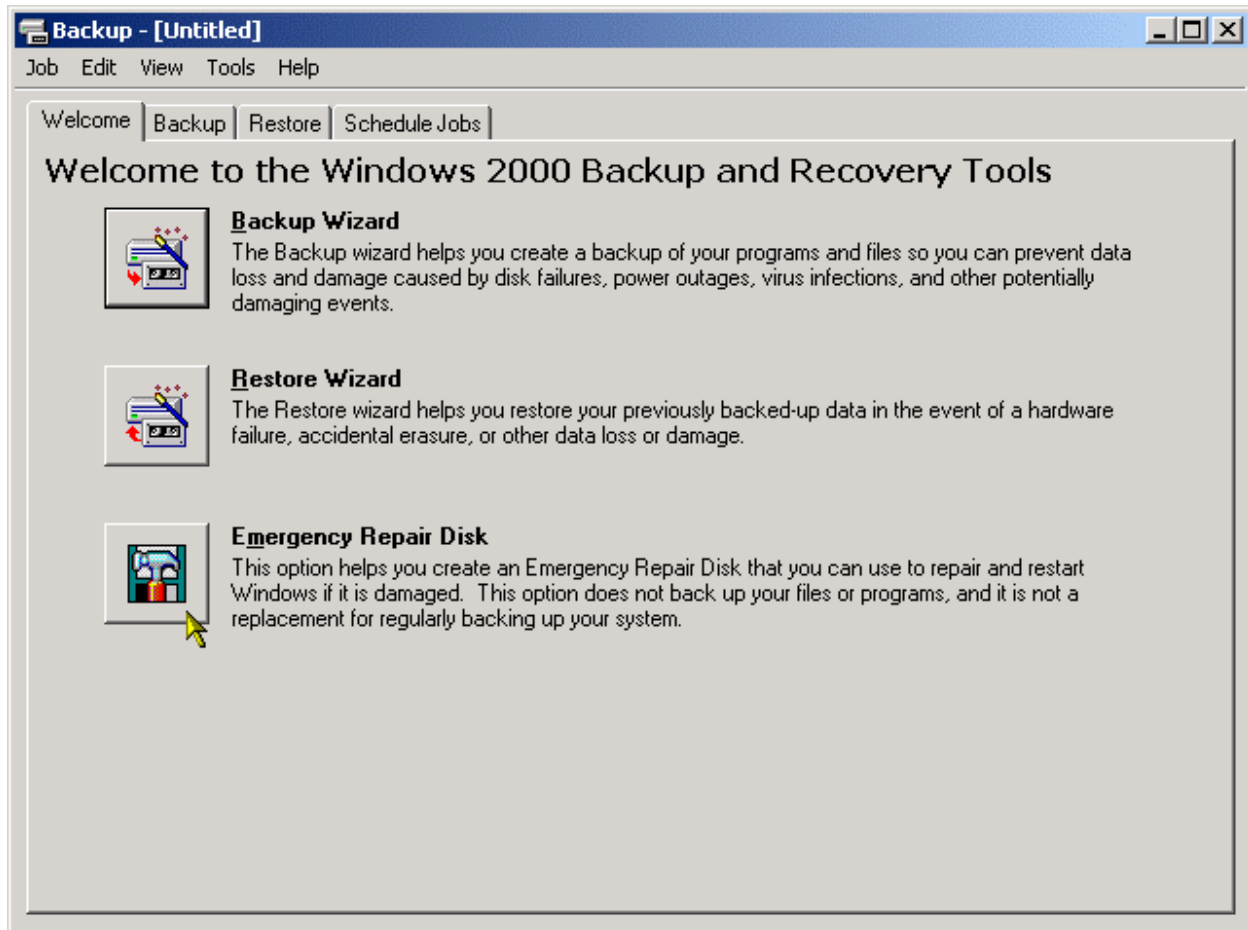


Figure 5.3: Using the Backup utility to create an ERD.

4. In the dialog box that appears, select the Also Back Up the Registry to the Repair Directory check box. (Selecting this option will overwrite anything in the repair folder.) Click OK.
5. Once the ERD is created and the Registry is copied to the repair folder, perform a full system backup. Make sure you include the System State. (I discussed backing up the System State in “Backing Up the System” earlier in this chapter.) This will completely back up the Registry and system and make sure that you can recover your system.

Using the Boot Loader Menu

When you attempt to recover a failed system, try using some of the options on the Boot Loader menu. In addition to the options included in the NT Boot Loader, Win2K offers a number of extras, as shown in Figure 5.4.

```
Windows 2000 Advanced Options Menu
Please select an option:

Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt

Enable Boot Logging
Enable VGA Mode
Last Known Good Configuration
Directory Services Restore Mode <Windows 2000 domain controllers only>
Debugging Mode

Boot Normally

Use ↑ and ↓ to move the highlight to your choice.
Press Enter to choose
```

Figure 5.4: Using the Boot Loader menu.

Here is what the menu options do:

- **Safe Mode**—Starts Win2K with the minimal set of drivers and services necessary to start Win2K.
- **Safe Mode with Networking**—Similar to Safe Mode but adds drivers and services necessary to enable networking.
- **Safe Mode with Command Prompt**—Similar to Safe Mode but starts Win2K with a Command Prompt window instead of Windows Explorer.
- **Enable VGA Mode**—Starts Win2K in VGA mode using the vga.sys driver instead of the regular video driver.
- **Last Known Good Configuration**—Starts Win2K using a previous version of the SYSTEM Registry hive. The Last Known Good Configuration is the most recent session that started successfully (without any service or driver-initialization failures) and allowed the user to log on to the computer.
- **Directory Service Restore Mode**—Allows you to recover the AD database. This option is valid only for Win2K domain controllers and requires you to set up a separate administrative password when you install AD.
- **Debug Mode**—Enables a startup mode in which Win2K sends debugging information across a serial cable to another computer running a debugger. (The mode uses COM2 as the debugging port.)
- **Enable Boot Logging**—Creates an extended log file of success and failure events for the initialization of system components as they load when Win2K starts up. (This behavior is the default for all safe-boot options except Last Known Good Configuration.) The log file is named nbtlog.txt and resides in the %Windir% folder (for example, C:\Winnt).

Using the Recovery Console

The *Recovery Console* allows you to attempt to recover or repair a Win2K system. It's a command-line service, so it has no GUI.

Win2K allows you to add the *Recovery Console* to the startup options for your system. Figure 5.5 shows the choices available to you once you choose *Recovery Console* from the Boot Loader menu. There are two installations of Win2K on devices on this computer. Unfortunately, it doesn't show you which versions are installed in which boot directory.

You can run the Recovery Console from text-mode Setup using the Windows 2000 installation CD-ROM or boot floppies, then choose *Repair* on the Welcome screen.

```
Microsoft Windows 2000(TM) Recovery Console.  
The Recovery Console provides system repair and recovery functionality.  
Type EXIT to quit the Recovery Console and restart the computer.  
  
1. C:\WINNT  
2. D:\WIN2K  
  
Which Windows 2000 installation would you like to log onto  
<To cancel, press ENTER>? _
```

Figure 5.5: Using the Recovery Console boot option.


This boot option allows you to quickly and easily start up in recovery mode. In recovery mode, you can carry out a number of useful functions, such as:

- Manage the state of services during the next startup (for example, enable or disable)
- Run CheckDisk (chkdsk.exe)
- Repair the boot sector using fixboot.exe
- Repair the master boot record (MBR) using fixmbr.exe
- Create and/or format drive partitions (which can be incredibly destructive to your recovery efforts)
- Perform numerous other functions to recover your system.

While the Recovery Console can help you recover file allocation table (FAT) and FAT32 subsystems, the significant feature is recovering NT file system (NTFS) partitions. This is important because many of us have likely run system partitions on FAT (we're afraid of being

left with a system that we cannot access in any simple fashion), allowing us to copy and delete files should an update or driver installation go bad. Of course, with Win2K and its deeper reliance on NTFS for many things, there is a persuasive reason to use NTFS for the system partition.


One important aspect of the Recovery Console is that you can boot to any installation of Win2K that exists on the system. This is fine for multi-boot installations, but it becomes really useful when you have mirrored drives installed. If one fails, you can still work on the other by booting to that instance of the OS.

 Also check Microsoft Knowledge Base article 229077, “When your system partition (containing the Ntldr, Ntdetect.com, and Boot.ini files) is part of a Win2K basic or dynamic disk software mirror, you cannot pre-install the Recovery Console,” at <http://support.microsoft.com/support/kb/articles/Q229/0/77.ASP>.

When you use the Recovery Console, you can access only the following folders:

- The %SystemRoot% folder (for example, C:\winnt)
- The c:\cmdcons folder (created when the Recovery Console is installed)
- Any folders on removable drives (for example, floppy disks or CD-ROMs).

No other folders are accessible; if you try to access them, an “Access Denied” error is displayed.

 In an interesting attempt at security, while you can copy files to the hard drive from other sources—for example, floppy disk or CD-ROM—according to Microsoft, you cannot copy files from the hard drive to other sources. This is the default security setting. You can, however, copy from one hard drive to the other, and this essentially gets around this issue.

If you want to enable all paths for the Recovery Console, you can do so by using one of the following tools to enable the SET command within the Recovery Console. (This is described in the Microsoft Knowledge Base article Q235364 at <http://support.microsoft.com/support/kb/articles/Q235/3/64.ASP>.)

- Security Configuration and Analysis MMC snap-in
- Domain Controller Security Policy in Administrative Tools
- Domain Security Policy in Administrative Tools
- Local Security Policy in Administrative Tools.

After you start one of these security tools (which one you use depends on your computer’s environment), locate the following two security policies under Local Policies\Security Options:

- Recovery Console: Allow Automatic Administrative Logon
- Recovery Console: Allow floppy copy and access to all drives and all folders.

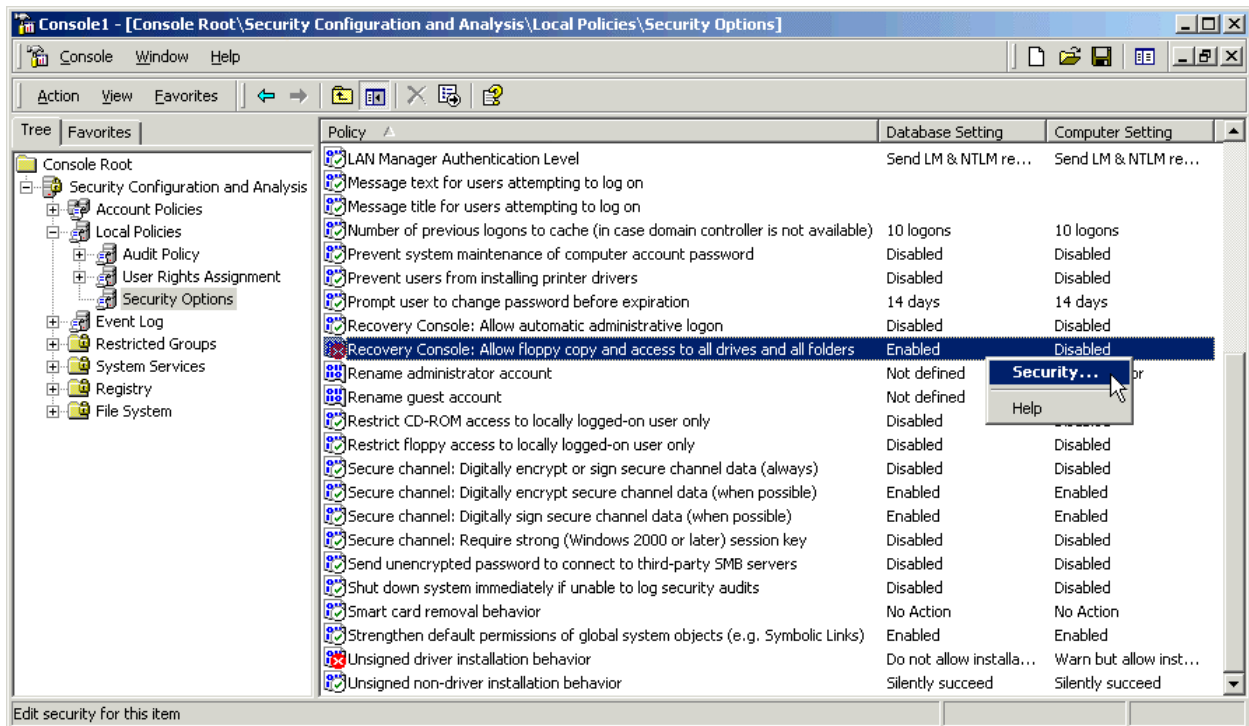


Figure 5.6: Security and Configuration Analysis options for the Recovery Console.

While the Recovery Console is only a command-line tool, it doesn't implement the full set of commands in the Command Prompt window you access in a full Win2K installation. To understand the limited set of commands available to you, see the Microsoft Knowledge Base article Q229716, "Description of the Windows 2000 Recovery Console," at <http://support.microsoft.com/support/kb/articles/Q2297/16.ASP>.

Adding the Recovery Console to the Startup Options

If you want to be able to start Win2K using the Recovery Console, you can add it as an option to the Boot Loader menu. Before you add it, make sure that you have:

- The Windows 2000 installation CD-ROM
- Logged in to the system with administrative privileges
- Approximately 7MB free on your system disk.

See Microsoft Knowledge Base article Q229077, available at <http://support.microsoft.com/support/kb/articles/Q229/0/77.ASP>. It states that when your system partition (containing the Ntldr, Ntdetect.com, and Boot.ini files) is part of a Win2K basic or dynamic disk software mirror/RAID-1 volume, specifically one created with the NT Disk Administrator or Win2K Drive Management MMC snap-in as opposed to a hardware-based RAID controller, you cannot pre-install the Recovery Console. If you want the Recovery Console pre-installed on a mirrored system partition to help facilitate a repair, you must break the mirror, install the Recovery Console, then re-establish the mirror.

To begin the installation:

1. Run the following command:

```
<cdrom>\i386\winnt32.exe /cmdcons
```

2. When the usual confirmation dialog box appears, click Yes. The installation process creates the C:\cmdcons folder, then copies the appropriate Recovery Console boot image and related files into it. The process also modifies the Boot.ini file and adds a new boot menu item:

```
C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows 2000 Recovery Console"  
/cmdcons
```

Once the Recovery Console is installed, a message is displayed, shown in Figure 5.6.

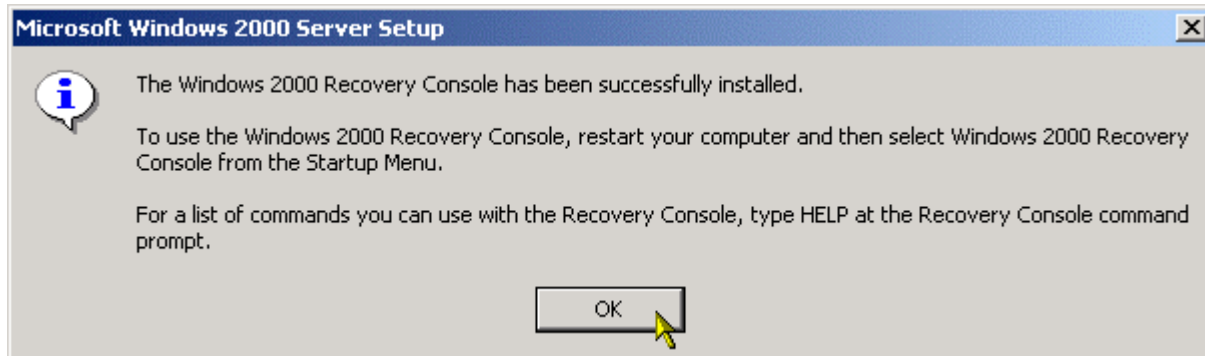



Figure 5.7: Successfully installing the Recovery Console.

3. Start up and select the Recovery Console option like any boot option.
4. Select an installation number; if applicable, select a specific instance of Windows.
5. Supply an Administrator password, which will be the Directory Services Restore mode administrator password you entered when you installed AD and made your computer a domain controller. Then the Recovery Console appears.

If only for convenience, I recommend installing the Recovery Console into each installation. If you install systems using unattended installations, use cmdlines.txt to add the following line. (Be sure to use the quotation marks, as discussed in Microsoft Knowledge Base article Q21641 at <http://support.microsoft.com/support/kb/articles/Q216/4/17.asp>.)

```
"<path>\winnt32 /cmdcons /unattend"
```

 A notable glitch in the Recovery Console is that it fails to run if you convert its host FAT16 or FAT32 volume to NTFS. The solution for this problem is to reinstall the Recovery Console using the same procedure you used to install it (that is, running Winnt32 /cmdcons).

Applying Updates, Patches, and Utilities

You need to keep up to date with Win2K updates and patches, and there are several Web sites where you can track them.

- <http://windowsupdate.microsoft.com/> —The Windows Update site (and the related Start menu item). However, this site will only get you so far because Microsoft doesn't release security patches to it immediately; it usually waits and tries to package a single installation containing several patches at a time.
- www.microsoft.com/security/ —The Microsoft Security site, which is more useful especially, although not specifically, for those servers facing the Internet. This site stores the bulletins in which Microsoft announces the latest issues, bugs, and security breaches against all its product lines. What's perhaps most important, you'll find patches released here before anywhere else.
- www.ntbugtraq.com/ —To keep up with Windows security bugs, I highly recommend checking out the NTBugtraq site. It's a mailing list for discussing security exploits and security bugs in NT and its related applications. It also held a lot of patches in its heyday, but this has become less of an issue now that Microsoft has improved its own site support.
- www.winternals.com/ —The excellent Winternals site is another good site for general utilities for Windows. It's dedicated to creating utilities that repair and recover Windows-based systems, allowing systems administrators to minimize both downtime and data loss. Winternals also provides a number of freeware utilities, and this gets them a good recommendation here.
- www.nsi.org/ and www.cert.org/ —The sites of the National Security Institute (NSI) and CERT Coordination Center (CERT/CC) are worth considering in the security area. For example, CERT/CC is the organization that grew from the computer emergency-response team formed by the Defense Advanced Research Projects Agency (DARPA) in November 1988 in response to the Internet worm incident. CERT/CC's charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, take steps to raise the community's awareness of computer security issues, and conduct research into improving the security of existing systems.

Service Packs and Patches—Why?

This chapter has discussed a number of maintenance, security, backup, and recovery issues. Managing these issues is critical to the ongoing success of your Win2K deployment. Although I've discussed numerous ways to track and manage support levels, security service packs, and patches, I haven't described the details of all the current issues because I wanted to focus on the methods rather than too many specifics. However, there is one serious issue that has recently come to light and that is an example of why these processes need to be followed.

There is a major bug in the AD backup and restore application programming interface (API) that likely affects a vast number of Windows 2000-based organizations. This bug was recently discovered by a number of parties, including the independent software vendor (ISV) Aelita Software, and publicized by Sean Daily, Senior Contributing Editor for *Windows 2000 Magazine* and Series Editor for Realtimepublishers.com.

The symptom of this bug is that although backing up AD seems to progress as expected, up to half of all backups may be corrupt and unusable. The corruption occurs in situations where two domain controllers are backed up simultaneously and one domain controller has an additional log file created during the process. (For additional details, see the Microsoft article mentioned below.) If you attempt to recover from a corrupt backup, you're likely to be left with a domain controller on which directory services cannot start.

Because Microsoft has provided standard APIs to access AD information, most backup solutions use these APIs to create their applications, yet the APIs are flawed. As a result, this issue affects not only the Win2K Backup utility and related System State backups but also third-party applications (for example, ARCserve 2000 from Computer Associates, Backup Exec from VERITAS Software, and ERDisk for Active Directory from Aelita Software). This is obviously a fundamental issue for any backup and recovery planning.

Unfortunately, reports indicate that there is usually no indication that this issue is happening until you attempt to restore AD. As Sean notes, "Affected backups are corrupted in such a way that when they're restored, they prevent the domain controller from starting and cause it to display a "Directory Service cannot start" error message. Also, in this situation, if you run NTDSUTIL using the Semantic Database Analysis option to run the database semantic checker, you receive error message 550: "Database is inconsistent." Using the Win2K Backup utility, the problem happens even when the Verify option is turned on."

Microsoft didn't initially admit that this issue existed. Although the problem appears to be fixed in Win2K SP2, little effort was made to publicize this, and there is strangely no mention of the fix in the SP2 release notes. On June 13, 2001, Microsoft finally officially acknowledged the problem in the Product Support Services article "Windows 2000 Domain Controllers Restored with System State Backups Made Prior to SP2 May Not Boot" (available at [//support.microsoft.com/support/kb/articles/Q295/9/32.ASP](http://support.microsoft.com/support/kb/articles/Q295/9/32.ASP)). Microsoft recommends applying a hotfix if you don't wish to upgrade directly to SP2, but you need to contact the company directly to obtain it. If at all possible, however, my advice is to patch the problem using SP2.

Finally, remember that although they're generally a good idea, not all hotfixes and service packs are a magic cure. Take, for instance, the botched release of E2K SP1, the installation of which had catastrophic effects for some organizations (including, in some cases, Exchange installations corrupted beyond repair or recovery). Simple common sense says that you need to test upgrades and patches in a test or quality assurance (QA) environment before applying them to your production environments. This includes testing your backup and restore procedures regularly as well as testing with live production backups to ensure that they're being created correctly.

Reviewing Security

Although you should already have completed a security audit and review of your installation, now is another good time to review your system for any potential security issues and ensure that all roles have been appropriately assigned, both in the policy of Win2K and in your organization.

I'm not going to discuss all security aspects of the Win2K environment in this section. Instead, I'll review where you are and emphasize the need for ongoing vigilance and review of your environment.

During the SANS99 and Federal Computer Security Conferences held in Baltimore from May 7 to 14, 1999, the SANS institute surveyed 1,850 computer security experts and managers. From this survey, it identified the "The 7 Top Management Errors that Lead to Computer Security Vulnerabilities." They're shown in Table 5.2.

This Error	Says the Experts Do This
Number 7	Ignore the problem and pretend it will go away.
Number 6	Authorize reactive, short-term fixes so problems re-emerge rapidly.
Number 5	Fail to realize how much money their information and organizational reputations are worth.
Number 4	Rely primarily on a firewall.

This Error	Says the Experts Do This
Number 3	Fail to deal with the operational aspects of security. They make a few fixes but don't allow the follow-through necessary to ensure that the problems stay fixed.
Number 2	Fail to understand the relationship of information security to the business problem. They understand physical security but don't see the consequences of poor information security.
Number 1	Assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job.

Table 5.2: “The 7 Top Management Errors that Lead to Computer Security Vulnerabilities.”

Consider these errors as you review your security. In Chapter 2 (“Assembling a Migration Team”), I suggested that when you formed your migration project team, you include security team members and communicate with them explicitly throughout the migration process. This approach allows you to review your security situation. By following the maintenance model, you should continue to regularly review security policy, services, and procedures.

This is too short a book to cover all aspects of security for Win2K, and there are many resources available to you to delve deeper into the fundamental security services offered by Win2K.

Keeping these concepts and issues in mind, lets take a look at the key things you can deal with now that your migration has progressed to ongoing support.

Securing Windows 2000

Installing Win2K servers is much more flexible than in NT 4.0. NT allowed you to install a server as a domain controller or member, and you could make only one change—promoting a member server to a domain controller. Win2K allows you to install the server as a domain controller or member server and change that role at any time—that is, you can promote or demote servers as required. While this change is available, it should obviously be used with care. The advantage is that you can reassess how many domain controllers you have in your new environment against how many you actually need.

In a base installation, default security is applied against users, groups, file, Registry DACLs (Discretionary ACL), and security policies. This is defined in the deflsv.inf template, which is located in the %systemroot%\system32\inf folder.

Users and groups installed on a member server are the same as for an installation of Windows 2000 Professional. Essentially, users and groups are still kept in a Security Account Manager (SAM) database. SAM is also stored in the Registry, further validating my previous discussion about the importance of backing up the Registry and related System State. When a server is joined to a domain, SAM remains, even if a server is promoted into the domain as a domain controller. However, this doesn't mean that you can access a domain controller server using locally stored credentials. When a server joins a domain as a domain controller, the local account database becomes unavailable for authentication or authorization; instead, you must use the domain database.

The issue you'll face is that unless you use AD to administer all servers' local policy, the local security policies will apply. The Local Security Policy (LSP) console controls these. However, while all servers maintain an LSP, it can be overridden by site, domain, and OU settings.

The default LSP for a server installation is similar to that used for Windows 2000 Professional, except for file and Registry permissions. The LSP is primarily in the following groups:

- Account policies
- Local policies
- Public key policies
- IP security policies.

You can manage these groups using the normal administration consoles or the Security Configuration and Analysis tool, which I'll discuss shortly.

Using Administration Tools

One of the final things to consider is how to manage your environment in a Windows 2000 Professional installation. While some tools are common to both Windows 2000 Server and Windows 2000 Professional installations, you must install some of the more advanced tools, such as the AD administration tools, separately to a Professional installation or member server. To do this, you need to use the Administrative Tools on the Windows 2000 Server CD-ROM.

Common Tools

These tools are provided in all installations:

- Computer Management
- Data Sources (ODBC)
- Event Viewer
- Performance
- Services.

You can use these tools to manage the related functions on the local computer. With the appropriate permission, you can also use them to look at other computers on the network and manage them remotely.

You may be familiar with the NT method of viewing event files remotely using Event Viewer, and in Win2K, the principle remains the same. Figure 5.7 shows one server connecting to another to view a remote log file. This is a very useful feature when you're looking for errors, such as replication errors, across new domains. Another situation would be monitoring for remote access or security breaches without having to visit the actual hardware.

In Event Viewer, the name of the local host is shown in parentheses at the root of the tree. Unfortunately, it shows only a single host in the list, so to monitor multiple hosts this way, you need to set up custom MMCs.

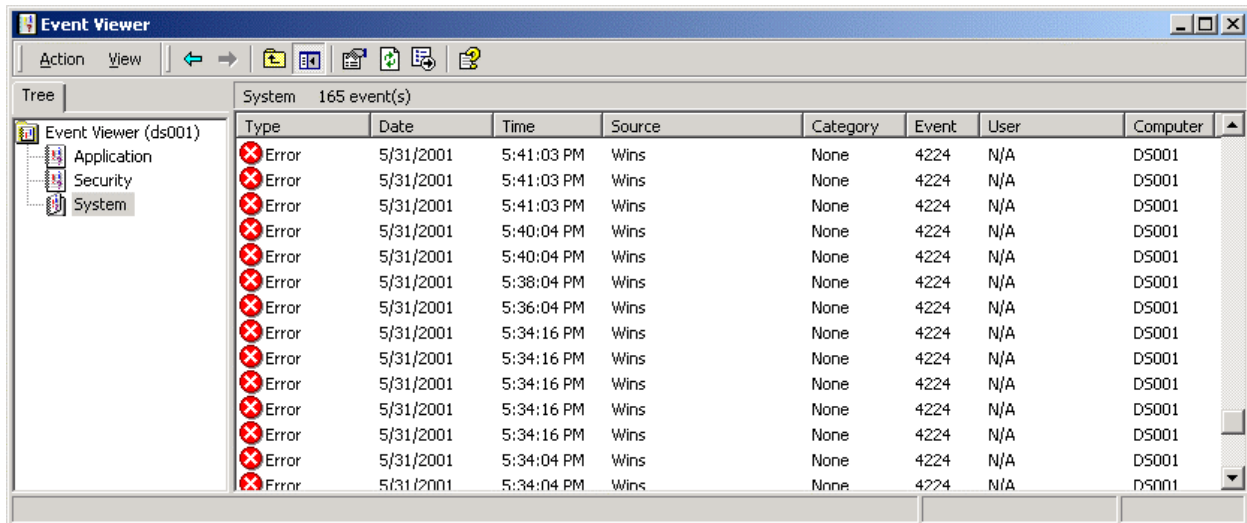


Figure 5.8: Reviewing event logs on a remote host.

Additional Tools

You can add the following tools to a Windows 2000 Professional or member server installation:


- Active Directory Domains and Trusts
- Active Directory Schema
- Active Directory Sites and Services
- Active Directory Users and Computers
- Certification Authority
- Cluster Administrator
- Connection Manager Administration Kit
- DHCP
- Distributed File Service
- DNS
- Internet Authentication Service
- Internet Services Manager
- QoS Admission Control
- Remote Boot Disk Generator
- Routing and Remote Access
- Telephony
- Terminal Services Manager

- Licensing and Client Connection Manager
- WINS.

These tools are all located in the i386 folder on the installation point. To install them, click the adminpak.msi file, and the Setup wizard will perform the installation. Unfortunately, this is an all-or-nothing installation for now, and you may end up with a bunch of tools you don't really need or want. Still, you can now manage your network without running server installations on your local computers.

You can use the Group Policy snap-in to publish or assign the Windows 2000 Administration Tools to other users or computers; the adminpak.msi file will then be automatically installed on those computers. (We discussed Group Policy extensively in Chapter 3.) To do this:

1. Group your users or computers in an appropriate OU, such as System Administrators.
2. Move the assigned administrator accounts into that OU.
3. Create and share a directory in which you locate the .msi application with at least read-only privileges—for example, \\adminserver\installshare.
4. Copy the .msi application (in this case, adminpak.msi) to the shared directory.
5. Create and edit a new GPO for the OU—for example, AdministratorToolsAssigned.
6. Using User Configuration|Software Settings, right-click the Software Installation settings, then select New from the shortcut menu.
7. In the File dialog box, type the full network path to the file—for example, \\adminserver\installshare\adminpak.msi.

 Remember to use share names only, not absolute file paths (for example, c:\installs). This is essential because file paths cannot be resolved across the network.

8. Click Open.
9. Either publish or assign the application.

As discussed earlier, the Windows 2000 Administration Tools is an extensive package of tools, and it may be more suitable to publish than assign.

- **Assign**—Administrative users will find the application folder called Administrative Tools on their desktops.
- **Publish**—Assignees can install the package on their workstations in a few easy steps: Choose Start>Settings>Control Panel. Double-click Add/Remove Programs, then select Add New Programs. Under Add Programs from Your Network, select Windows 2000 Administration Tools, then click Add.

Using Security Tools

The Windows 2000 Resource Kit, as with previous versions of Windows, offers a wide range of utilities. A set of Support Tools is also included with Windows 2000 Server.

Security Configuration and Analysis Tool Set

The Security Configuration and Analysis tool set allows you to review the current configuration of installations against predefined templates to check for conformance and change the installation, if required. This tool set has three components:

- The default Security Template MMC snap-in
- The Security Configuration and Analysis MMC snap-in (also known as Security Configuration Editor and Security Configuration Manager), shown in Figure 5.8
- The secedit.exe tool.

Because the first two components are MMC snap-ins, you add them to a console in the standard way; secedit.exe is a command-line tool.

The SCA tool set is similar to the one offered in the NT 4.0 Resource Kit. It allows you to:

- Load the default security templates and apply them to computers
- Audit a computer for compliance against those templates
- Define templates using the full set of security options available and save them as your own defaults (password and access policies, local audit policy, user rights and lockout policy, hardware security options, Registry settings, system services startup options, and much more).

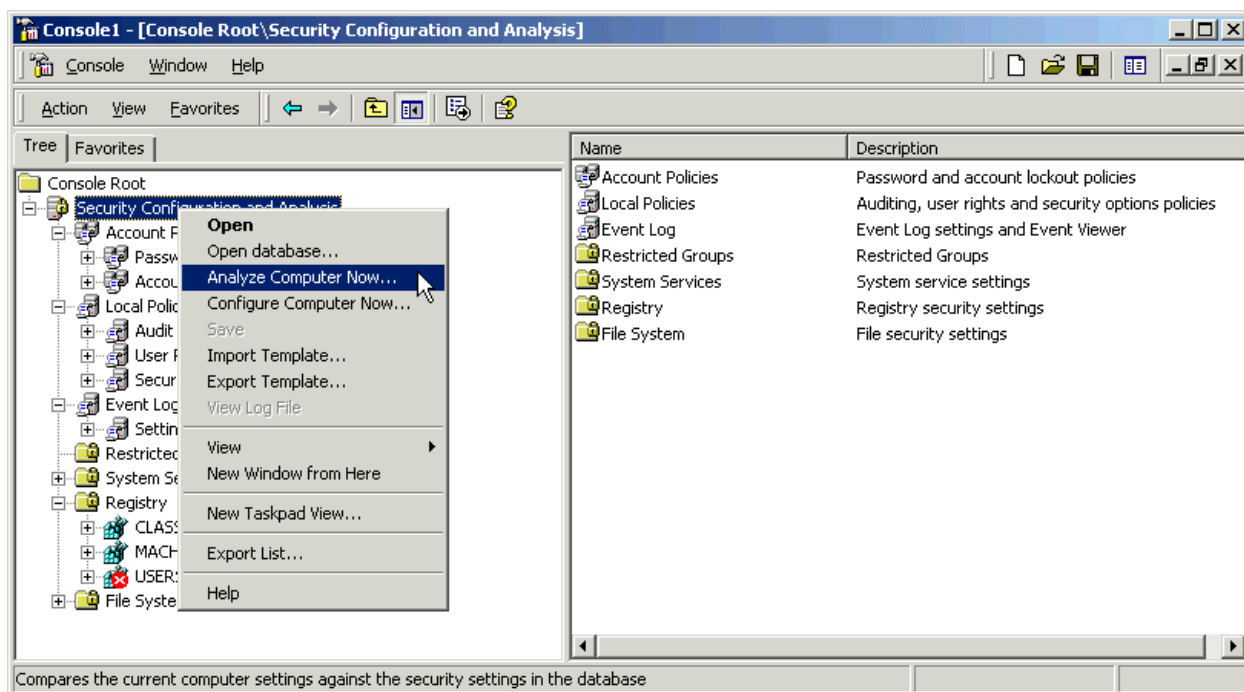


Figure 5.9: Using the Security Configuration and Analysis tool set in the Windows 2000 Resource Kit.

Moving beyond the current computer, the secedit.exe tool allows you to build batch files, which you can implement across a distributed network. Alternately, you can import the templates into Group Policy, then apply them across a site, domain, or OU. This greatly enhances your ability

to administer your domain environment, while at the same time decreasing the amount of effort you have to put in.

Internet Security Systems System Scanner

Another very interesting tool is the Internet Security Systems (ISS) System Scanner. If you're familiar with ISS tools, you'll appreciate this addition.

System Scanner for Windows is a security-assessment solution for Win2K, NT 4.0, Windows 95, and Windows 98. While I found some false reports (for example, it reported no virus scanner installed, when I actually did have one installed), it performs nearly 300 vulnerability checks, including:

- Extensive system-baseline capabilities, including file, Registry, and user
- Browser-specific vulnerabilities
- Comprehensive IIS/PWS (Internet Information Server/Peer Web Services) checks
- Presence of well-known Transmission Control Protocol/Internet Protocol (TCP/IP)-based services
- Network Basic Input/Output System (NetBIOS) checks
- Java vulnerabilities
- Microsoft Office vulnerabilities
- Windows 95 Policy Editor misconfigurations
- Susceptibility to denial of service attacks
- Configuration of virus scanners
- Registry security checks
- User policy configuration checks
- Remote-access checks and modem checks.

System Scanner allows you to define your own policies and schedule scans to run at specified times. Easy-to-use HTML reports provide detailed descriptions of vulnerabilities detected on your computer and the information necessary to correct them.

System Scanner isn't provided when you install the Windows 2000 Resource Kit; you need to install it yourself. You can do this easily by double-clicking *syssscansetup.exe* in the apps\systemsscanner folder of the Windows 2000 Resource Kit companion CD-ROM, then following the instructions on the screen.

Other Tools

The Windows 2000 Resource Kit contains a number of other tools, but the documentation for the basic installation runs over 1,000 pages, so this isn't the place to review all of them. However, I reviewed several tools in Chapter 4 that are useful to the migration process. (See "Migration

Tools and Techniques.”) I highly recommend that you take a look at the Resource Kit and related security tools for your own environment.

At the end of this book, I’ll take a look at a selection of third-party tools for security, along with the more general migration tools.

Summary

So ends the first section of this book and my review of migrating from NT 4.0 to Win2K. As I said at the beginning of this section, this book was intended to be one of the most concise guides to migration to Win2K and E2K, and I hope you’ll agree that a lot of key information has been condensed into the first five chapters.

Now it’s time to look at one of the most germane reasons to migrate to Win2K—and that is E2K—and this is what the next section is devoted to. Although I’ve given a simple review of the features of E2K so far, you’ll likely spend a lot of time considering it as a key benefit of migrating to Win2K, especially if you already have Exchange 5.x installed.

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.