ITPro™ SERIES

Windows & .NET MAGAZINE eBooks

Migrating to Windows Server 2003, Active Directory, and Exchange 2003

By Dan Holme and Dan Balter

Contents

Chapter 5

Maintaining Windows Server 2003 in a Post-Migration Environment

After migrating your directory services to Windows Server 2003 Active Directory, you are ready to leverage Active Directory for more effective management of your enterprise network. This chapter will jump-start administrators who are new to either Windows Server 2003 or Active Directory. We will examine key concepts and procedures that affect day-to-day administration of users, groups, computers, and permissions.

Preparing for the Administration of Windows Server 2003

After migrating, you will want to familiarize yourself with the suite of administrative tools available for Windows Server 2003 and provide those tools to appropriate administrative personnel.

Native Administrative Tools

You will immediately notice a new Start menu, which is also called the Start panel. The administrative tools reside in several places:

- Start menu
- All Programs menu
- Control Panel

If you do not see the Administrative Tools folder in the Start menu or the All Programs menu, or if you want to control when and where the folder appears, then follow this next procedure:

Customize the Location of the Administrative Tools Folder

1. Right-click the Start button and choose Properties.
2. Click the Customize button.
3. Click the Advanced tab.

4. Scroll down to the System Administrative Tools option group and select the option that meets your needs: *Display on the All Programs menu, Display on the All Programs menu and the Start menu* (i.e., the default selection), or *Don't display this item.*

The Administrative Tools folder remains visible in the Control Panel, unless you use policy settings to modify the behavior of the Control Panel.

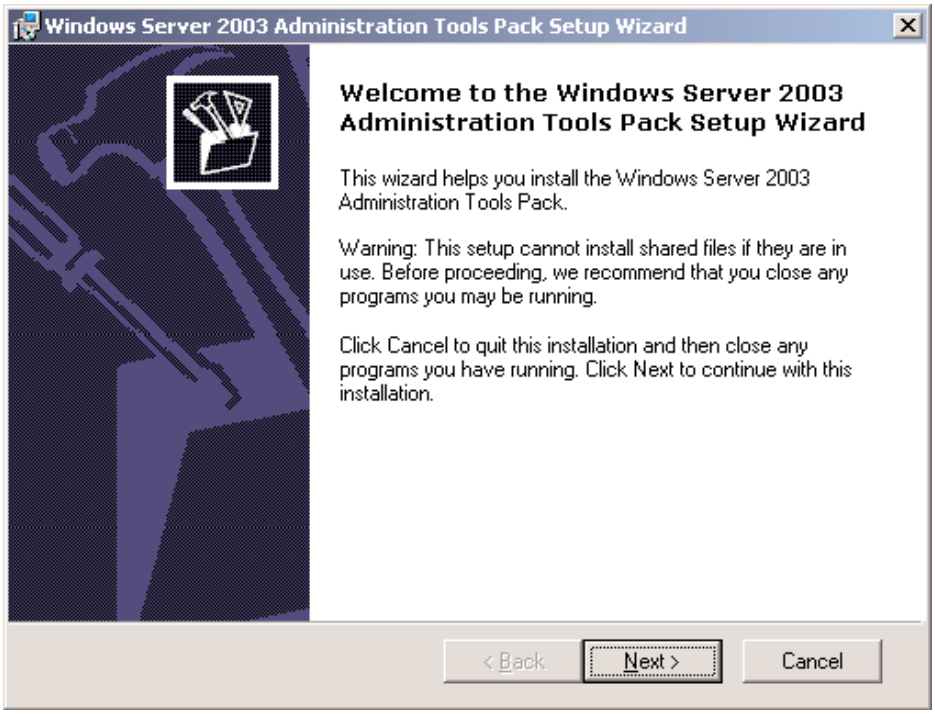
The default administrative tools on Windows XP Professional and Windows 2000 Professional are sufficient for managing the client system, but don't come close to providing the comprehensive toolset you need to support an enterprise Windows network. For example, you will need tools to support servers, services, and Active Directory.

Install the Full Suite of Native Administrative Tools

To install the Windows Server 2003 Administration Tools Pack (adminpak.msi) on a Windows XP Professional Service Pack 1 (SP1) or later client, open the adminpak.msi file, which is in the I386 folder of the CD-ROM. The Windows Installer package is also available in the System32 folder of a computer running Windows Server 2003. To access this folder remotely, administrators of the server can connect to *servername*\admin$\system32. The wizard, which Figure 1 shows, will guide you through the installation of the administrative tools.

Figure 1:

Viewing the Windows Server 2003 Administration Tools Pack Setup Wizard



You can install Windows Server 2003 Administration Tools Pack on Windows XP Professional SP1 or later and Windows Server 2003 systems, but not on Windows 2000 systems. The tools are backward compatible so you can use them to administer any Windows Server 2003 or Windows 2000 Server system. The tools include enhanced functionality, such as the drag-and-drop feature, and additional useful utilities. You can use most, but not all, of these new features to support Windows 2000 Server.

Keep the following notes in mind:

- You can install the Windows 2000 adminpak.msi on only Windows 2000 machines and use it to administer only Windows 2000 servers and domain controllers (DCs).

- Adminpak.msi is typically updated with service packs, so you should install the latest version of the administrative tools that matches your service pack level.
- Client, tool, and server matching is required in a few situations. In other words, when performing certain tasks remotely, you must use a Windows 2000 client running the Windows 2000 administrative tools against a Windows 2000 server. Similarly, you must perform certain tasks with a Windows XP or Windows 2003 client running the Windows 2003 administrative tools against a Windows 2003 server.

Tip

In a mixed Windows 2000 Server and Windows Server 2003 environment, your best bet is to use Windows XP SP1 or later with the Windows 2003 Server Administration Tools Pack to administer your enterprise. For those rare occasions when you run into limitations, use Remote Desktop to administer your Windows 2000 Servers or have available a Windows 2000 client with Windows 2000 administrative tools.

The information we provided earlier should be sufficient to get you running effectively with the full suite of native administrative tools. However for more information and for support with any problems, we recommend that you refer to these additional resources:

Note

For more indepth information regarding the ins and outs of cross-platform remote administration, see the Microsoft article, "Administering Windows Server-Based Computers Using Windows XP Professional-Based Clients," at http://support.microsoft.com/default .aspx?scid=kb;en-us;304718.

Note

For details about Windows 2003 administration and scripting, see the Microsoft Windows Server 2003 Resources Web site at http://www.microsoft.com/technet/prodtechnol /windowsnetserver/proddocs/server/strategies_and_tools.asp and the Microsoft article, "How to use Adminpak.msi to install a specific server administration tool in Windows," at http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B314978.

Introduction to the Microsoft Management Console

Windows administrative tools share a common framework called the Microsoft Management Console (MMC). (For more information about the MMC, see the Microsoft Management Console Center Web site at http://www.microsoft.com/windows2000/technologies/management/mmc/.) The MMC displays tools in a customizable window with a left pane that displays a tree structure (similar to the Windows Explorer tree) and a right pane that displays details.

Tip

The one thing to remember about the MMC is that you *right-click* to do everything. Although the MMC provides menus, they are not conveniently positioned and are not administrator friendly.

Tools or *snap-ins* use the two-paned console to provide administrative functionality. Snap-ins cannot run as standalone tools; they can function only within the context of the MMC.

Familiar Snap-ins

Most native administrative tools, which are available in the Administrative Tools folder, are one console with one snap-in. If you have supported Windows NT 4.0, then you will recognize several of the native consoles, such as Event Viewer. Some tools have had minor modifications, including the Performance tool.

The new Performance console has the functionality of earlier Performance Monitor versions divided into two snap-ins: one that graphically shows performance from realtime measurements or log files and one that creates and manages logs and alerts.

Tools Relocated to the MMC Framework

As with any change in technology, half the fun is finding the things you are familiar with. For example, you'll see that the old Services applet from the Windows NT Control Panel is now the Services snap-in, which is in the default Services console called Services.

New Snap-ins and Consoles

One of the tools you will use most often to support a Windows enterprise is Active Directory Users and Computers. This snap-in lets you administer common objects in Active Directory.

Note

To launch the Active Directory Users and Computers snap-in, select Start, Run, then type the filename dsa.msc.

Super Consoles with Multiple Snap-ins

Microsoft has provided a particularly powerful console, the Computer Management console. Computer Management is the *super console* to use to do just about anything to a system. You'll notice it contains multiple snap-ins, including some of those we've already seen as standalone consoles:

- Event Viewer
- Performance Logs and Alerts
- Services

Computer Management also contains numerous, highly-useful snap-ins such as:

- Shared Folders
- Local Users and Groups
- Device Manager
- Disk Management
- Disk Defragmentation

And this super console contains snap-ins to administer services installed on the local machine, including Microsoft Internet Information Server (IIS).

Tip

You will use Computer Management often, so memorize the shortcut: Right-click My Computer and select Manage.

Creating Simple Customized Consoles

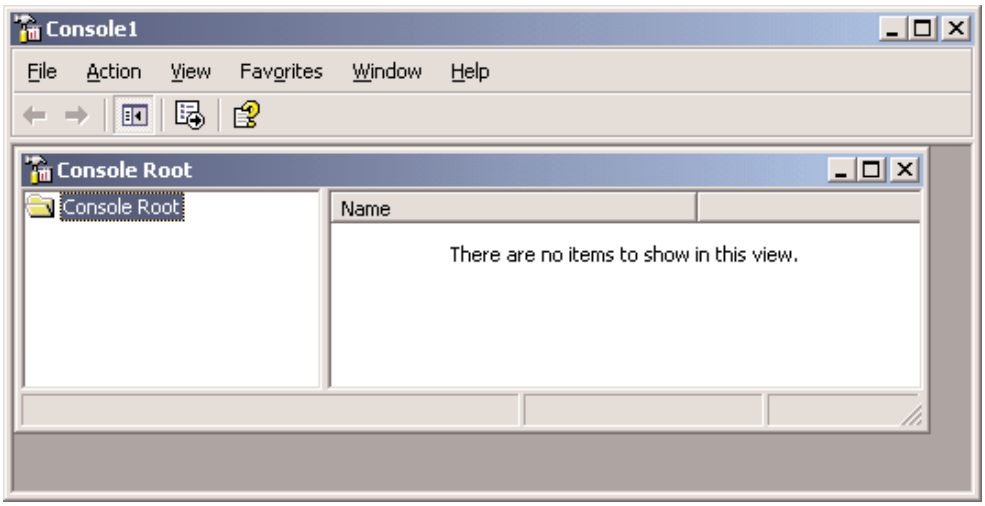
An important benefit of the MMC framework is that you can create customized consoles with shortcuts, Web pages, file-system access, and task pads that focus on the specific systems and duties for which you are responsible.

Create a Simple Customized MMC Snap-in

1. Choose Start, Run, and MMC. The empty MMC appears, as Figure 2 shows.

Figure 2:

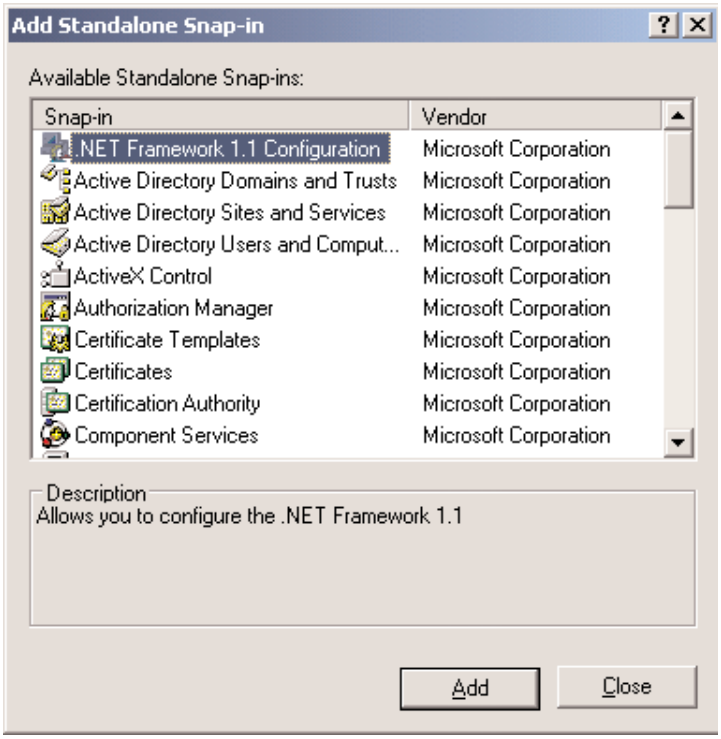
Showing the Empty MMC



2. Choose File, then Add/Remove Snap-in. The Add/Remove Snap-in dialog box opens.
3. Click Add.

The Add Standalone Snap-In dialog box (which Figure 3 shows) appears, listing the snap-ins installed on your computer.

Figure 3:
Viewing the Add Standalone Snap-in Dialog Box

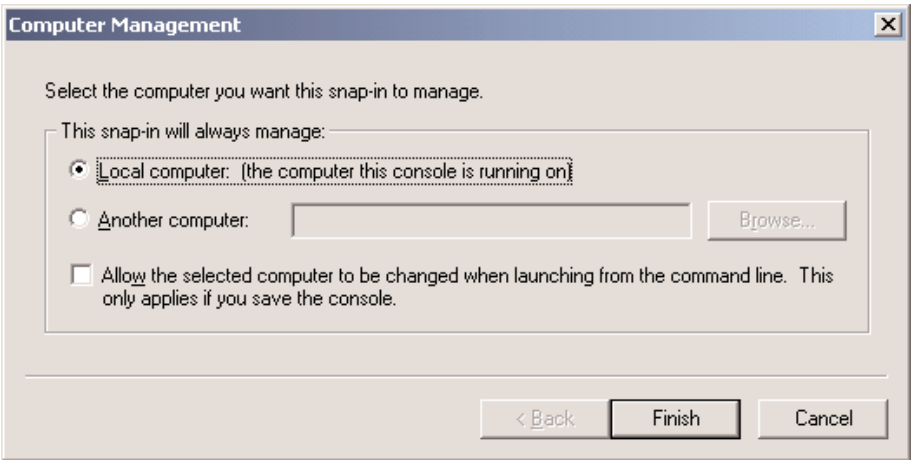


Note

If you only see a partial list, then some administrative tools have probably not been installed on the system. Don't forget to install the Administration Tools Pack (adminpak.msi).

4. Select a snap-in.
5. Click Add.
6. Many snap-ins will then give you additional options, including the ability to select the *focus* of the snap-in (i.e., the computer to which the snap-in will connect). Figure 4 shows the selection to manage a local computer. Make your selections and click Finish.

Figure 4:
Selecting Snap-in Options in the Computer Management Dialog Box



7. When you've added all desired snap-ins, click OK in the Add/Remove Snap-in dialog box.
8. Select File, then Save to save the snap-ins.

Snap-ins are saved as small .msc files, which specify the console configuration. Their small size makes them easy to distribute (for example, through email applications).

The default save location is the Administrative Tools folder of your user profile. The path to the folder is not intuitive.

Note

By default snap-ins are saved in the %userprofile%\Start Menu\Programs\Administrative Tools folder.

You can save an .msc file wherever you want, but the default location lets your custom snap-ins follow you when you have implemented a roaming user profile for yourself (which we highly recommend for administrators). However, snap-ins will function properly only when run on a system that has had the appropriate administrative tools installed on it.

The default location for saving Administrative Tools unveils a design flaw in Windows Server 2003. The custom snap-ins you create are not available in the Administrative Tools folder in Control Panel or on the Start Menu. They are available only in the Administrative Tools folder in the All Programs menu.

Other Important Administrative Tools

The native Windows Server 2003 administrative tools provide basic functionality that will support your environment, but additional tools that are available free of charge will further augment your capabilities.

Support Tools

The Windows Server 2003 CD-ROM includes many useful utilities and documents in the Support folder.

Note

Support tools are usually updated with service packs and reside in the Support folder of the service pack CD-ROM. Make sure to install the tools that match your system's service pack level.

Among the most valuable support tools are:

- ADSI Edit
- Setup Manager
- Replication Monitor

and several command-line tools (such as netdom.exe and netdiag.exe) to enhance your scripting and administration.

Group Policy Management Console

We examine the Group Policy Management Console (GPMC) below in the Group Policy section. You will definitely want to install the GPMC on the systems you use to manage Group Policy.

Resource Kit

Intermediate and advanced administrators will find it impossible to live without the Windows Server 2003 Resource Kit Tools. The Resource Kit is available from multiple sources including from the Microsoft Download Center at http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en.

Service-Specific Administrative Tools

Of course you will want to install tools that are specific to the services you support, such as Microsoft SQL Server, Microsoft Exchange Server, Microsoft Systems Management Server, Microsoft Acceleration Server, IIS, or Lotus Notes. The installation and use of these tools falls outside the scope of this discussion.

Remote Desktop

All Windows Server 2003 installations include a license for two concurrent connections to the server when using Remote Desktop for Administration. This technology, formerly called Windows 2000 Server Terminal Services, provides an administrator full access to the server and its installed tools, applications, and services.

Configuring Remote Desktop for Administration

Remote Desktop for Administration is installed by default on Windows Server 2003, but you must enable Remote Desktop Connections (RDCs) before administrators can begin to connect remotely to a server.

Enable Remote Desktop for Administration

1. Right-click My Computer and choose Properties.
2. Click the Remote tab.
3. Select *Allow users to connect remotely to this computer*.

On a DC, members of the DC's builtin Administrators group are allowed to use Remote Desktop for Administration to connect to the server. On member servers, members of the server's Remote Desktop Users local group are allowed to connect to the server. Modify membership of these groups to establish which users are permitted to use Remote Desktop for Administration.

The Client Side

A Windows Server 2003, Windows XP, or Windows 2000 system can use the Remote Desktop client to connect to a Windows Server 2003 server.

Install the Remote Desktop Client

The Terminal Services or Remote Desktop client must be installed. The client can be installed on Windows Server 2003, Windows XP, or Windows 2000 computers.

The Remote Desktop client installer package is named msrdpcli.msi. It resides in the *servername*\admin$\system32\clients\tsclient\win32 folder on a Windows Server 2003 computer.

Tip

The client also installs the Remote Desktops snap-in, which lets you build a custom MMC with direct *remote desktop* connections to the servers that you administer. We recommend you build a custom administrative console that includes the Remote Desktops snap-in.

After installing the client, you might discover that is hard to *find* because it is buried. Go to Start, All Programs (or Programs in Windows 2000), Accessories, then Communications to uncover it. We recommend you copy the shortcut to your desktop or some other easily accessible location. To connect to a server, simply open the client and enter the server's name or IP address. The client provides options that let you configure session properties, display size, etc.

Managing RDCs

As mentioned earlier, Remote Desktop for Administration supports two concurrent connections. When an administrator is finished performing tasks that require a RDC to a server, it is important that the administrator *log off* the server. By logging off, the administrator releases the connection so that another administrator can use it. If the administrator simply disconnects the session (by closing the Remote Desktop client window or by selecting the Disconnect option), then the session remains active and the connection is not available for other administrators. If an administrator attempts to connect to a server and both of its connections are taken, then the administrator will not be able to log on to the server. You can manage remote connections to minimize and troubleshoot such scenarios.

End a User's RDC to a Server

Sometimes you might try to use Remote Desktop for Administration to connect to a server and receive a message that no connections are available. You can use the Terminal Services Manager console to connect to a server and examine the sessions that are active on the server.

1. Open Terminal Services Manager from the Administrative Tools folder.
2. If you do not see the server listed that you want to manage, then right-click the All Listed Servers node and choose *Connect to computer*.
3. Select the server you want to manage and ensure the Users tab is visible.
4. Right-click the connection that you want to manage and choose *Log off*.

Note

Logging off a user session will close all active processes in the session and can result in the loss of unsaved data. Use the Reset command only when a session has become unresponsive.

Configure Remote Desktop Session Behavior

You can configure the server so that inactive or disconnected sessions are automatically logged off.

1. Open Terminal Services Configuration from the Administrative Tools folder.
2. Click the Connections node in the tree pane.
3. Double-click RDP-Tcp in the details pane.
4. Click the Sessions tab.
5. Select *Override user settings*.
6. Modify the settings to reflect your desired configuration.

Note

The most common problem with Remote Desktop for Administration is that administrators finish their task and disconnect, rather than log off. To address this problem, set the *Idle session limit*, select the second *Override user settings box*, then select *End session*. Remember that ending a session closes all processes and can result in the loss of unsaved data.

Using Alternate Credentials (aka Secondary Logon or Runas)

Most administrators log on using their administrative account. This practice is dangerous because the account has access to much more of the network than a standard user account. Thus a virus or trojan horse can cause significant damage—in fact administrators are often the biggest culprit in spreading viruses that do serious damage to an enterprise network.

To avoid this problem and other problems like it, don't log on as an administrator. Instead, log on as a standard user and use the Run As feature to launch administrative tools in the security context of an administrative account.

Run a Program with Administrative Credentials

1. Shift+right-click the shortcut for an executable, Control Panel applet, or MMC snap-in that you want to launch and choose *Run as*.
2. Select *The following user*.
3. Type the username (in the format *domain\username* if the account exists in a different domain) and password of the administrative account you want to use. When using the local Administrator account, enter the account as *machinename*\Administrator.
4. Click OK.

Other Run As Options

You can also configure shortcut properties so that you will be prompted for alternate credentials when you use the shortcut. To do this, right-click the shortcut, choose Properties, click the Advanced button, then select *Run with different credentials*.

Finally, you can use the Runas command from the Run box or command shell. For Help, open the command shell and type

```
runas /?
```

Important Notes About the Runas Command

- If you use Runas to try to run a program from a network share, you might encounter credential errors because the credentials used to connect to the share are in effect.
- If Runas fails, the Secondary Logon Service might not be running.
- For more information, see Windows Help.

Tip

An extremely important best practice for administrators and support personnel is to maintain at least two accounts: a user account with rights, privileges, and permissions common to other users in the enterprise, and an administrative account with rights, privileges, and permissions necessary to perform appropriate administrative tasks. To log on administrators should use their user account, then use Runas and their administrative credentials to launch administrative tools.

Note

For more information about the Runas command, see the Microsoft article, "Step-by-Step Guide to Using Secondary Logon in Windows 2000," at http://www.microsoft.com /technet/prodtechnol/windows2000serv/howto/seclogon.asp.

Models for Providing Administrative Tools

There are several popular ways to provide administrative tools to appropriate personnel:

- Distribute the tools and install them directly on computers that administrators use. Remember that Windows Server 2003 administrative tools run on only Windows XP SP1 or later and Windows Server 2003 computers.
- Provide the Remote Desktop Client to administrators, and let them connect directly to the servers to perform administrative tasks. Remember that a server supports only two concurrent connections in the Remote Desktop for Administration mode.
- Install administrative tools on a server running Windows Server 2003 and use Terminal Services to let multiple administrators connect to the server with the Remote Desktop.
- Install administrative tools on a desktop running Windows XP SP1 or later, then use a third-party tool to provide remote access to the administrative desktop. Tools such as Virtual Network Computing (VNC) or Symantec pcAnywhere can provide remote access to a Windows XP desktop to multiple administrators.

Select the method that meets your needs most effectively. If you do not implement Windows XP on the desktop, then you cannot distribute Windows Server 2003 administrative tools directly to administrators and will likely need a remote desktop administrative model. If you do not use Windows XP and you have many administrators, then Remote Desktop for Administration's two-connection limit might not suffice, so you might need to implement Terminal Services to provide administrative tools.

Active Directory Administration 101

Many organizations migrate to Windows Server 2003 that have little or no experience administering Active Directory. Even though you are familiar with the concepts of users, groups, and computers, you might be less familiar with how to use the new directory service and its administrative tools to manage those objects. This section will give you the skills you need to perform day-to-day administrative tasks in the new environment.

Tip

In the event that you are already familiar with fundamental administrative tasks in Active Directory, we recommend you skim this section and look at the items identified as tips (with formatting similar to this paragraph). You will find some tips that can enhance your productivity.

User Accounts

To manage user accounts, you can use the Active Directory Users and Computers snap-in.

Create a User Account

1. Open Active Directory Users and Computers.

2. Expand the domain node and drill down to the organizational unit (OU) where you want to create the user account.
3. Right-click the OU and choose New, then User.
4. In *First name*, type the user's first name.
5. In *Initials*, type the user's middle initial.
6. In *Last name*, type the user's last name.
7. Modify *Full Name* when necessary.
8. In *User logon name*, type the name that the user will log on with and (from the drop-down list) click the UPN suffix that must be appended to the user logon name following the @ symbol.

Note

Usernames in Windows 2000 can contain some special characters (including periods, hyphens, and apostrophes), which let you generate accurate usernames.

9. If the user will logon from Windows NT, Windows 98, or Windows 95 computers with a different name, then change the user logon name as it appears in *Downlevel logon name* to the different name.
10. Click Next.
11. Enter the user's initial password in both password boxes.

Tip

We recommended selecting *User must change password at next logon* so that the user can create a new password unknown to the IT staff. Appropriate support staff can always reset the user's password at a future date if they need to log on as the user or access the user's resources. But only users should know their passwords on a day-to-day basis.

12. Click Finish.

After a user has been created, the user object contains dozens of properties you might want to configure. To configure user properties, right-click the user and choose Properties.

Manage a User Object or *Account*

To perform almost all common administrative tasks on user objects, you right-click the user object and select the appropriate command from the shortcut menu. Among the commands available on the shortcut menu are:

- Rename
- Reset password
- Disable (when the account is currently enabled)

- Enable (when the account is currently disabled)
- Add to group

Unlock a User Account

If a user attempts to log on with an incorrect password, a logon failure is generated. When too many logon failures occur within a short period of time, the account is locked on the assumption that an intruder is attempting to penetrate the account by trying various passwords. Later we examine the Account Lockout policy that drives this behavior.

If a user account is locked out, the user will be notified when they attempt to log on. The message that appears clearly states that the account is locked out (not that an incorrect username or password was entered). To unlock a user account:

1. Right-click the user account and select Properties.
2. Click the Account tab.
3. Clear the checkbox labeled *Account is locked out.*

Groups

To manage groups, you can use the Active Directory Users and Computers snap-in.

Create a Group

1. Open Active Directory Users and Computers.
2. Expand the domain node and drill down to the OU where you want to create the group.
3. Right-click the OU and select New, then Group.
4. Type the name of the new group. (By default, the name you type is also entered as the downlevel name of the new group.)
5. Select the Group type and scope. For information about group type and scope refer to the later section.
6. Click OK.

When you create a group, you must specify the group's type and scope.

Group Type

Distribution and security are the two types of groups.

Distribution Groups

Distribution groups are used with email applications. These groups are not security enabled—they do not have Security Identifiers (SIDs)—so they cannot be given permissions to resources. Sending a message to a group sends the message to all members of the group.

Security Groups

Security groups are security principals and have SIDs. These groups can be placed in access control lists (ACLs), and therefore can be used to control security for resource access. Security groups can *also* be used as a distribution list by email applications.

Note

Most organizations use only security groups, because they fill both email and security requirements.

Group Scopes

Global, domain local, and universal are the three group scopes. Each group scope has unique characteristics related to the types of objects that can be members and the replication of the group, which affects their availability for use in ACLs.

Domain Local Groups

Domain local groups are designed to manage *resource access* within a domain. For example, when users in an organization need access to a high-speed printer, you can create a High-Speed Printer Users domain local group and give appropriate permissions to the printer. Then you can add users to the group, and through their group membership they will have access to the printer.

Domain local groups can contain user accounts, global groups, and universal groups from its domain or any trusted domain. In native mode, domain local groups can also contain other domain local groups.

Domain local groups replicate within the Domain naming context (NC). They are not available outside of their domain. So domain local groups can be members of only domain local groups in their domain and can be placed in ACLs in only the same domain.

Global Groups

Global groups are designed to *identify collections of users* in a single domain. Their members share a common characteristic such as job function, location, or departmental membership. For example, a global group can identify the SalesReps, the SalesManagers, and the FinanceManagers users in an organization.

Global groups can include accounts from only the same domain as members. In mixed mode, global groups can contain only users from the same domain. In native mode, global groups can include other global groups as members—for example, a Management group can include both the SalesManagers and FinanceManagers global groups.

To provide permissions to resources, you can add global groups to domain local groups. For example, both the SalesManagers and FinanceManagers might require access to the high-speed printer. You can add them both to the High-Speed Printer Users group. This process is much easier than adding each individual user to the High-Speed Printer Users group.

Job function, geography, and other identifying criteria usually do not map one-to-one with resource access needs. The existence of global and domain local groups lets you easily identify users and easily manage those users' resource access.

Global groups replicate to the global catalog, but their memberships do not. All domains in the forest, and all trusting domains, can use global groups as members of their domain local and universal groups. Other domains can also place them in ACLs, but this is not best practice.

Universal Groups

Universal groups are used to identify *users* in a *multidomain forest*. Universal groups are available as security groups in a native mode domain and can contain user accounts, global groups, or universal groups from any domain in the forest. A universal group can be used to collect global groups from

multiple domains in a forest. For example, a universal Engineers group might contain the global engineering groups from multiple divisions and domains.

Then universal groups can be placed into an ACL or (as a better practice) nested into a domain local group anywhere in the forest. Universal groups are replicated entirely in the global catalog, including both the group name and the membership. Therefore, you should keep the membership of universal groups fairly static and to a minimum. A universal group that contains only groups, and not individual user accounts, will meet these criteria.

Local Groups

Local groups are not created in Active Directory. To create local groups, you use the Local Users and Groups snap-in. Then they are stored in the SAM database on member servers and workstations. DCs do not support local groups. These groups might sound familiar because they are just like those in Windows NT 4.0.

Note

In native mode when you use domain local groups, you will most likely use only the builtin and default local groups and not create or manage any custom local groups.

Nesting

Nesting, or adding a user or group to another group, simplifies administration and reduces replication traffic. You can nest user accounts and groups in any combinations that the rules mentioned earlier allow.

For example, if we want to give permission to the 35 accountants in the accounting department to the Accounts Payable and Accounts Receivable folders, we can create individual access control entries (ACEs) to do so. Imagine the nightmare of adding the account of every new user who joins our company to the ACL of every resource to which they must have permission. Best practice dictates that we use nesting to simplify our lives. When a new accountant joins the firm, we simply add the user's account to the global Accountants group, which is nested in all the domain local groups necessary to ensure proper permissions to the resources accountants need.

The best practice for nesting in Windows Server 2003 domains at Windows 2000 native functional level or higher is:

Note

User accounts should go into
Global groups, which in turn go into
Domain Local groups with
Access permissions to the appropriate resource.

In a multidomain Active Directory forest with domains set to Windows 2000 native functional level or higher, the guidelines we provided earlier outline the best practice. When using universal groups, remember the following note, which provides additional guidelines:

Note

User accounts should go into
Global groups, which may go into
Universal Groups, which in turn can go into
Domain Local groups with
Access permissions to the appropriate resource.

Adding Users to Groups

Although you can add users to groups and manage the membership of groups in several ways, we will discuss three options:

- From the user object, select Properties and the Member Of tab.
- From group object, select Properties and the Members tab.
- From user object, right-click and select Add Members To A Group.

In any of these cases, a Select dialog box appears to let you choose the appropriate group or user.

Tip

A very important tip is to learn the best way to use the Select dialog box. Type the first few letters of the user or group and click OK. Then a short list of accounts will display from which you select the exact object you want. When you type enough letters to uniquely identify the account, the tool will select it correctly and automatically.

Remember that access is granted by comparing the ACL to the user's security token, which is generated at logon and includes the user's SID and SIDs representing each group of which the user is a member.

Tip

When a user or group is added to a group, each must reauthenticate to add the SID from the new group to its token.

Computer Objects

Computers in an Active Directory domain are *security principals* which means, like users, they have an account (an object in Active Directory) with an internal username and password and, of course, a SID. Like a user, a computer uses its account to authenticate, audit, and access domain resources.

Creating Computer Accounts

The following can add computers to the domain:

- Domain Administrators can add computer accounts to a domain.

- Authenticated Users can add 10 computer accounts to a domain. This ability is controlled by the ms-DS-MachineAccountQuota attribute, which you can change using ldp.exe or ADSI. Users cannot use this capability to add workstations with Microsoft Remote Installation Services (RIS). With RIS, users must have permissions to create child computer objects for the OU in which the computer will be added.
- Any user with the permission to create child computer objects on an OU can add a computer account.

Create a Computer Object or Account

1. Open the Active Directory Users and Computers snap-in.
2. Right-click the OU or container in which you want to add the computer.
3. Choose New, then Computer.
4. Type the computer name.

After a computer object has been created, it contains properties you might want to configure. To configure computer properties, right-click the computer and choose Properties.

Manage a Computer Object or Account

To perform almost all common administrative tasks on user objects, you right-click the user object and select the appropriate command from the shortcut menu. Among the commands available on the shortcut menu are:

- Reset
- Disable (when the computer object is enabled)
- Enable (when the computer object is disabled)
- Move
- Manage

Tip

When you choose Manage, the Computer Management console opens and focuses on the computer. This console provides a very slick way to begin remote administration of that computer.

Joining to a Domain

After you have created the computer object in Active Directory, you need to join the computer to the domain.

Join a Computer to a Domain

1. Log on to the computer with credentials that belong to the local Administrators group on the computer.

Note

Only local administrators can alter the domain or workgroup membership of a computer.

2. Open the System applet:
   - Right-click My Computer and select Properties.

   Or
   - Choose Start, Settings, Control Panel, then System.
3. Click the Network Identification tab (Windows 2000) or the Computer Name tab (Windows XP).
4. Click Properties (Windows 2000) or Change (Windows XP).

Note

On Windows 2000 systems, avoid the evil Network Identification Wizard, which forces you through multiple steps to accomplish what you can do quite easily from the Properties dialog box.

5. Under *Member of*, click Domain.
6. Type the name of the domain you want to join.

Tip

Use the full DNS name of the Active Directory domain. This practice is this more accurate and more likely to succeed, and when using this practice, a failure indicates a problem with DNS name resolution that you should rectify before joining the machine to the domain.

7. Click OK.

If the computer does not yet have an account in the domain, you will be prompted to provide *domain* credentials that have sufficient privileges or permissions to create a computer account.

8. Click OK to close the System Properties dialog box.

Now use the procedure below to provide the correct domain credentials to create a computer account:

1. A user with *local administrator* credentials logs on to the machine.
2. The administrator uses the System applet in Control Panel to direct the machine to join a domain.
3. The computer locates a DC for the target domain.

Note

This step is often the weakest link in the process, so when you have any problems joining a domain, suspect and troubleshoot DNS name resolution first.

4. The domain requests *domain* credentials to authenticate the user.
5. The domain checks (based on the computer's name) to see if an object or account already exists for the computer.
6. If not, the domain confirms that the user (domain account) has sufficient permissions or privileges to join a workstation to the domain and creates an object for the computer in the default Computers container.
7. The computer assumes the identity of its Active Directory object. It configures its SID to match the domain computer account's SID and sets an initial password with the domain.
8. The computer performs other tasks related to joining the domain. It adds the Domain Admins group to the local Administrators group and the Domain Users group to the local Users group.
9. You are prompted to reboot the system.
10. The next time the system starts, you will have the opportunity to log on to your domain account.

Tip

The very first time you start a computer that has just joined the domain (including newly *imaged* systems), you need to click the Options button in the *Log on to Windows* dialog box and select the appropriate domain from the *Log on to* drop-down list.

Managing Group Policy

In Windows NT 4.0, security settings (e.g., user rights), policies (e.g., password policy), and configuration of the computer and user environment were managed using disparate tools. With the introduction of Windows 2000, Microsoft consolidated much of this administration into the framework of Group Policy—a fundamental component of change and configuration management in Microsoft's newer OSs. Now, hundreds of settings can be configured centrally for one or multiple systems or users. Settings are pulled automatically by Group Policy client-side extensions that operate on each computer running Windows 2000 or later.

This section provides sufficient coverage to enable you to use default Group Policy Objects (GPOs) to manage the most important policy settings. For a comprehensive discussion of Group Policy we recommend, "Group Policy, Profiles and IntelliMirror for Windows 2003, Windows 2000 and Windows XP," by Jeremy Moskowitz.

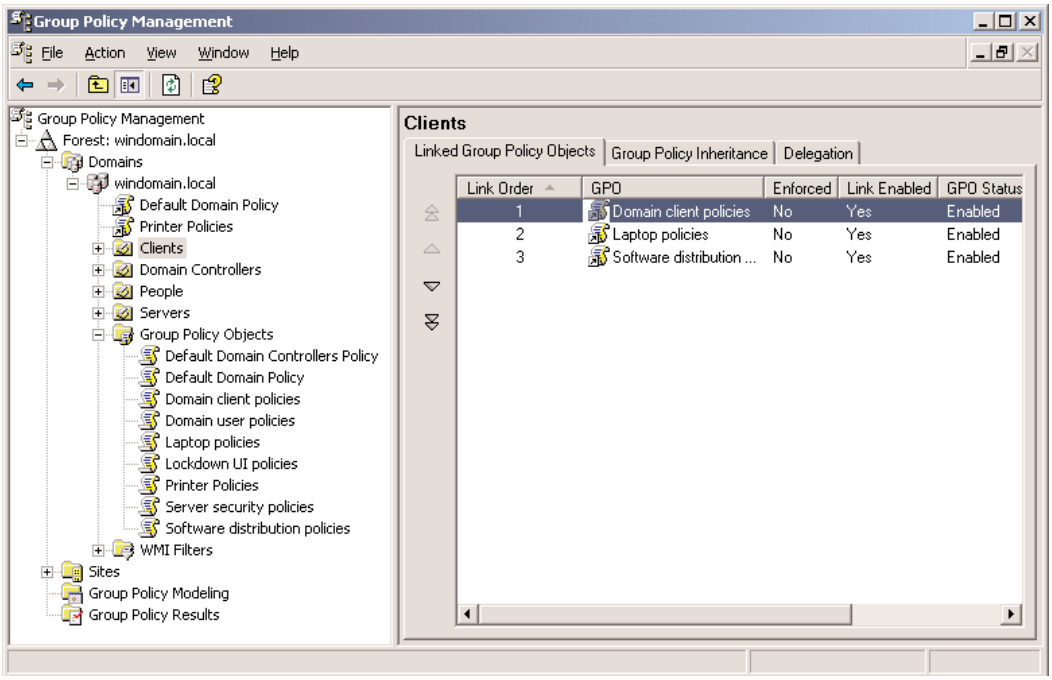
Installing the GPMC

To manage Group Policy most effectively use the appropriately-named GPMC—a new MMC snap-in that centralizes and facilitates the creation, linking, application, management, and analysis of GPOs. In Windows 2000, you can administer GPOs only from the Properties dialog box of a site, domain, or

OU. And the UI makes locating and understanding options related to the application and functioning of the GPO difficult.

The GPMC, which Figure 5 shows, provides one interface with drag-and-drop functionality to enable an administrator to manage Group Policy settings across multiple sites, domains, or even forests. Some of the capabilities of GPMC include the ability to backup, restore, import, and copy GPOs, while providing an intuitive reporting interface displaying GPO deployment. For example, using this tool an administrator can easily determine exactly which GPOs apply to a given domain, how inheritance settings are configured, and which users or groups have been delegated the ability to manage these objects. The GPMC is available for download from Microsoft at http://www.microsoft.com/windowsserver2003/gpmc/default.mspx.

Figure 5:
Displaying the GPMC



Group Policy Terminology and Concepts

Over the years, Microsoft has honed its use of terminology related to change and configuration management—and Group Policy in particular. This section will introduce you to fundamental Group Policy concepts and terminology.

The goal of change and configuration management is to centralize the administration of the user and computer environment in your enterprise. This goal includes controlling application availability, security configuration, and the behavior and availability of system features for specific users or computers.

Policy Settings

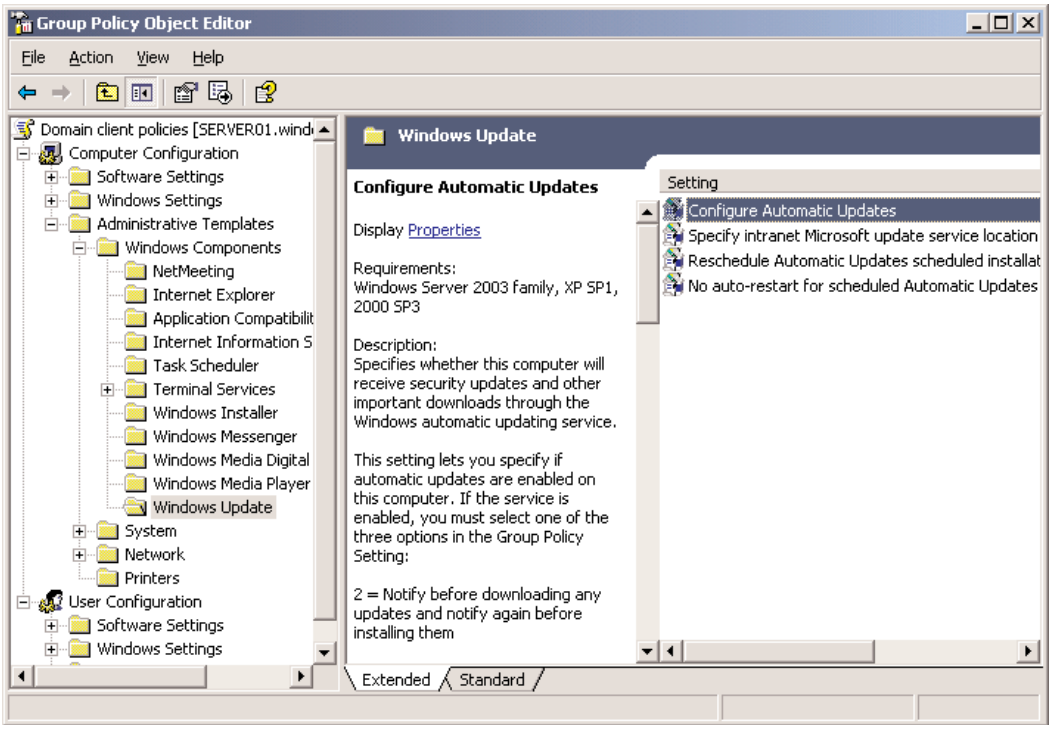
You will be interested in the configuration of a specific setting or feature at the most granular (i.e., most detailed) level. Group Policy represents the configuration as a *policy setting*: an individual setting that determines a specific configuration. A commonly cited policy setting is the *Remove Run from Start menu* policy setting. As its label describes, after enabling this policy setting, the Run command does not appear on the Start menu.

A policy setting can be *enabled*, *disabled*, or *not configured*. When a policy setting is either enabled or disabled, it can determine the configuration of the element it controls. You must be careful about interpreting policy settings, because you can end up with single-, double-, and even triple-negative situations. For example, when you *disable* the setting *Remove Run from Start menu*, you are in fact ensuring that the Run command *does* appear on the Start menu. When a policy setting is not configured, it has no affect on the configuration of the computer or user environment. This rule is important because you will likely end up with an environment that is configured by more than one GPO. If a policy setting is enabled (or disabled) in one GPO and is not configured in another GPO, then the first GPO determines the resulting configuration.

GPOs and the GPO Editor

Policy settings are collected in GPOs. To configure the policy settings in a GPO, you use the GPO Editor, which Figure 6 shows. To launch the GPO Editor, right-click a GPO and select Edit. Policy settings are organized into two top nodes: Computer Configuration and User Configuration. Computer Configuration policy settings are applied by a computer at startup. User Configuration policy settings are applied by a computer when a user logs on. As you drill down into each node, you will find a hierarchy of folders that organize hundreds of policy settings. By default, each policy setting in a new GPO is set to *not configured*.

Figure 6:
Using the GPO Editor to Configure Policy Settings



Many policy settings include explanatory text, which displays in the left side of the details pane (as Figure 6 shows) or on the Explain tab of the policy setting's Properties dialog box. Almost all policy settings appear either in the Computer Configuration *or* the User Configuration node because they either affect a computer (regardless of which user is logged on) or a user (regardless or which computer the user is logged on to). A few policy settings appear in both nodes of a GPO. In those cases, the policy's explanation text will tell you how the two settings interact when both are configured.

Tip

If a GPO contains policy settings only in the User Configuration or Computer Configuration node, we recommend disabling settings in the unused node. Select the GPO in the GPMC, click the Details tab, and use the GPO Status drop-down list. By disabling the unused node of the GPO, you will improve GPO processing because the client-side extensions will not attempt to evaluate that GPO when applying user or computer policy settings.

A GPO can configure (enable or disable) one policy setting or many policy settings. To learn what policy settings are configured in a GPO, select the GPO in the GPMC and click the Settings tab.

GPO Scope

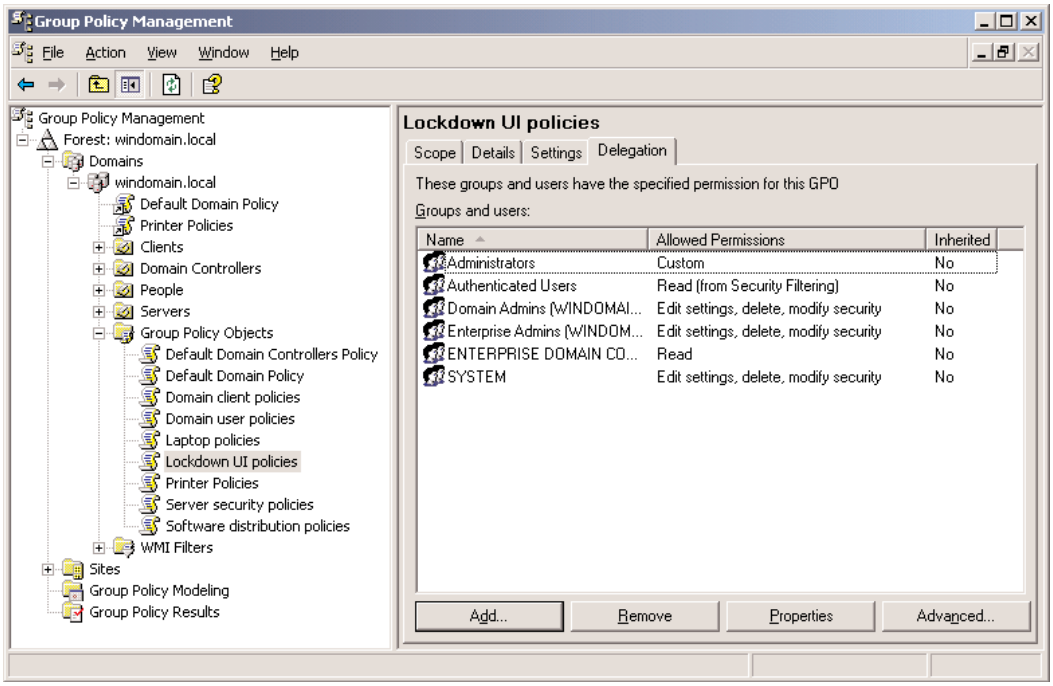
The computers or users that are affected by a policy setting are within the *scope* of the GPO containing the policy setting. A GPO can be *linked* to one or more Active Directory sites, domains, or OUs. After a policy is linked to a site, domain, or OU, the users or computers in that container are within the scope of the GPO. Select a GPO and click the Scope tab to identify the containers to which the GPO is linked.

You can further refine the scope of a GPO by filtering the scope of the GPO. You have two ways to filter the scope: through security filtering or Windows Management Instrumentation (WMI) filtering.

Security Filtering

The first way to filter the scope, Security filtering, involves modifying the *delegation* (i.e., permissions) of the GPO. To administer GPO permissions, you use the Delegation tab of a GPO in the GPMC, as Figure 7 shows. The Apply Group Policy permission of a GPO determines the security filtering of a GPO. When a user or computer is within the scope of the GPO and the Apply Group Policy permission is set to Allow, the GPO will apply to that user or computer. By default, the Authenticated Users group is granted Allow (Apply Group Policy), meaning that all users and computers within the GPO's scope are governed by the policy settings in that GPO.

Figure 7:
Displaying the Delegation tab of a GPO in the GPMC



By modifying this permission, you can reduce the effect of the GPO. For example, when a policy is linked to the domain, but you do not want the policy to apply to the Managers group, you can add a permission Deny (Apply Group Policy) to the Managers group. As you know from Windows NT 4.0, a deny permission overrides an allow permission, so that all users (i.e., Authenticated Users) will apply the policy except for those who belong to the Managers group.

Alternatively, to specify that *only* users (or computers) in a particular group should be affected by a GPO, *remove* the Allow (Apply Group Policy) permission that is assigned to the Authenticated Users group. By doing so, the GPO will not apply to any users or computers. Then add a group and grant it Allow (Apply Group Policy). The GPO will affect only users and computers in that group.

WMI Filtering

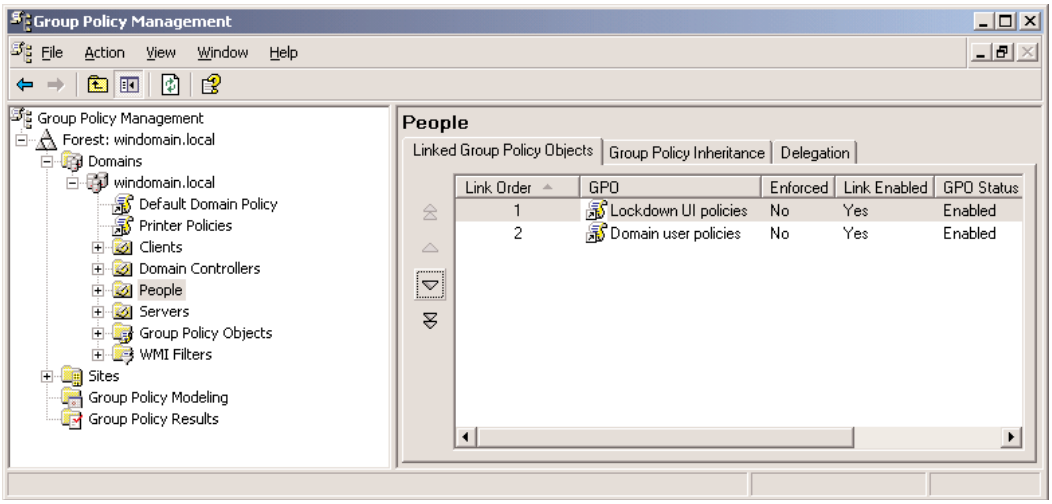
The second way to filter the scope of a GPO is through WMI filtering. WMI filters can detect and respond according to a system's characteristics. For example, you can configure a WMI filter that applies a GPO only when a computer has sufficient free disk space or when a computer is running a particular OS or service pack.

GPO Precedence and Inheritance

A policy setting can be configured in more than one GPO, and GPOs can be in conflict with one another. For example, a policy setting can be enabled in one GPO, disabled in another GPO, and not configured in a third GPO. In this case, the *precedence* of the GPOs determines which policy setting the client applies. A GPO with higher precedence will win over a GPO with lower precedence. Whether the policy setting is enabled or disabled in a GPO with higher precedence, the configured setting takes effect. However, if the policy setting is not configured in the GPO with higher precedence, the policy setting (either enabled or disabled) in the GPO with lower precedence will take effect.

A site, domain, or OU can have more than one GPO linked to it. The *link order* of GPOs determines the precedence of GPOs in such a scenario. GPOs with higher-link order take precedence over GPOs with lower-link order. When you select an OU in the GPMC, the Linked GPOs tab shows the link order of GPOs linked to that OU, as Figure 8 shows.

Figure 8:
Selecting the Linked GPOs Tab to Review Link Order



The default behavior of Group Policy is that lower-level containers inherit GPOs linked to a higher-level container.

Note

When a computer starts up or a user logs on, the Group Policy client-side extensions examine the location of the computer or user object in Active Directory and evaluate the GPOs with scopes that include the computer or user. Then the client-side extensions apply policy settings from these GPOs. Policies are applied sequentially, beginning with the policies linked to the site, followed by those linked to the domain, followed by those linked to OUs—from the top level OU down to the OU in which the user or computer object exists. This sequential application of GPOs creates an effect called inheritance.

By default, inherited GPOs take lower precedence than GPOs linked directly to the container. In a practical example, you might configure a policy setting to disable the use of registry-editing tools for all users in the domain by configuring the policy setting in a GPO linked to the domain. All users within the domain will inherit that GPO and its policy setting. However, you probably want administrators to be able to use registry-editing tools, so you will link a GPO to the OU that contains administrators' accounts and configure the policy setting to allow the use of registry-editing tools. Because the GPO linked to the administrators' OU takes higher precedence than the inherited GPO, administrators will be able to use registry-editing tools. As you can see from this simple example, the default order of precedence ensures that the policy that is *closest* to the user or computer wins.

Precedence can be further complicated because a container can be configured to Block Inheritance. For example, when an OU is blocking inheritance, GPO application begins with any

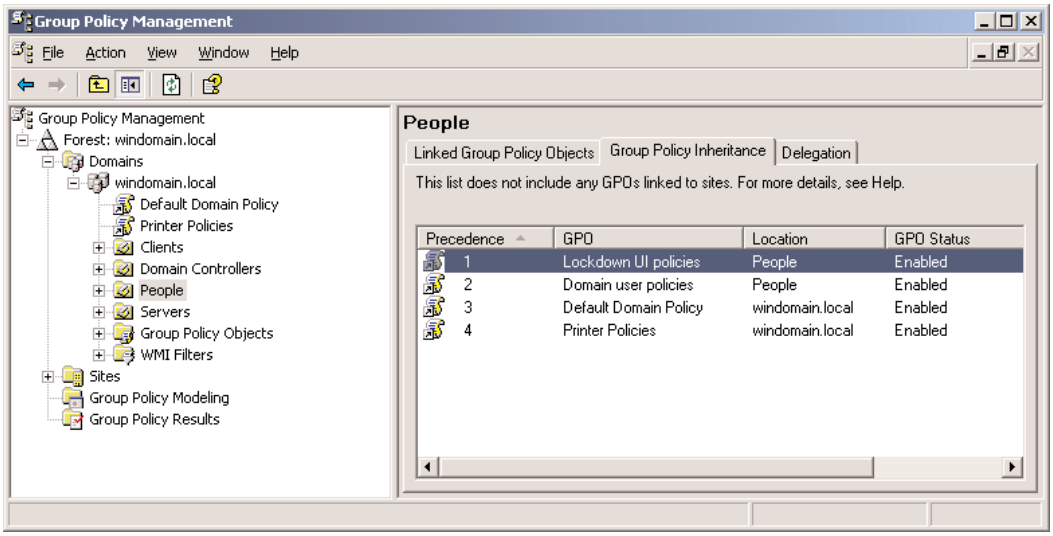
GPOs linked directly to that OU—GPOs linked to higher-level OUs, the domain, or the site will not apply.

In addition, a GPO link can be enabled (the default), disabled, or set to Enforced. To do this, right-click a GPO link, as Figure 9 highlights. When a GPO link is set to Enforced, the GPO takes the highest level of precedence—policy settings in that GPO will win over any conflicting policy settings in other GPOs. In addition, a link that is Enforced will apply to child containers even when those containers are set to Block Inheritance.

To facilitate evaluation of GPO precedence, you can simply select an OU (or domain) and click the Group Policy Inheritance tab, as Figure 9 shows. This tab will display the precedence in effect, accounting for GPO application, link order, inheritance blocking, and GPO link enforcement. This tab does not account for policies that are linked to a site, nor does it account for GPO security or WMI filtering.

Figure 9:

Reviewing the GPO Status from the Group Policy Inheritance Tab



Resultant Set of Policies

Because a GPO can contain many policy settings, each of which can be enabled, disabled, or not configured, and because multiple GPOs with various scopes and filters exist in your enterprise, ascertaining what will happen to a user or computer can be difficult. The settings that end up applying to a user or computer—based on the user or computer's location in Active Directory, the GPOs that contain the user or computer in their scope, security filters, WMI filters, GPO status, link order, inheritance, and enforcement—are called the Resultant Set of Policies (RSoP).

The GPMC provides two graphical tools with which to analyze RSoP: the Group Policy Modeling Wizard and the Group Policy Results Wizard. To access either wizard, right-click the appropriate node

in the GPMC. You will find a full discussion of these tools in the book by Jeremy Moskowitz, which we mentioned earlier.

Creating and Linking GPOs

To use the GPMC to create a GPO, right-click a site, domain, or OU to which you want to link the GPO and choose Create and Link a GPO Here. Alternatively, right-click the Group Policy Objects container and choose New.

To link an existing GPO to a site, domain, or OU, click the Group Policy Objects container and drag a GPO from the details pane to the appropriate container. To delete a GPO link, expand the site, domain, or OU containing the GPO link, then select the link and press the Delete key. To delete a GPO, expand the Group Policy Objects container, select a GPO and press the Delete key. When you delete a GPO, you are deleting it entirely; a deleted GPO will no longer be linked to any of the containers it was previously.

Default Domain Policy

The Default Domain Policy GPO determines several important policy settings. The Default Domain Policy is linked to the domain responsible for configuring the password and account lockout policies for the domain, as well as Kerberos and certificate policies. Using the Default Domain Policy GPO to configure these policies—and only these policies—is a best practice. Do not create another GPO to configure these policies. Conversely, do not use the Default Domain Policy GPO to configure any other policies .

As we mentioned in the discussion about Active Directory design, a domain can have only one password, lockout, Kerberos, and trusted Certificate Authority (CA) policy. A common mistake is for administrators to create GPOs linked to OUs and attempt to configure password policies, which is not possible—such GPOs determine the password policies only for *local* accounts on computers in the OU, not on domain accounts.

For example, if you have a situation in which some users require long passwords and others require short passwords, then you will need to have two domains or use a third-party utility to manage that requirement.

Default Domain Controller Policy

The Default Domain Controller Policy GPO is linked to the DCs OU and controls the computer configuration for machines in that OU. Keeping all DCs in the DCs OU, and refraining from putting other computer accounts in the OU, is a best practice. By segregating DCs in an OU with a policy linked to it, you can ensure consistent configuration of DCs across the enterprise.

The Default Domain Controller Policy GPO specifies many security settings including auditing and user rights. By default, DCs are more secure than member servers because they have a more limited set of logon rights and privileges. To generate a full report of the settings in the Default Domain Controller Policy GPO, select the GPO in the GPMC and click the Settings tab.

The best practice is to configure all DC-specific settings in the Default Domain Controller Policy GPO, so you have an authoritative source of settings specific to DCs.

Member Server and Workstation Policies

Windows Server 2003 provides no default GPO to configure policies on member servers and workstations. You can use the procedures mentioned earlier to create a GPO linked to an OU that contains computer accounts for member servers, workstations, or both. Configure policy settings in the GPO, and those settings will apply to computers in that OU and in child OUs.

Among the most useful nodes in a GPO are the User Rights Assignment node and the Security Options node, which are in the Computer Configuration\Windows Settings\Security Settings\Local Policy folder. These two nodes contain many of the policy settings that you configured using User Manager and Server Manager in Windows NT 4.0.

Managing File and Folder Access

As discussed in earlier chapters, file and folder permissions are called ACEs and are collected in the discretionary ACL (DACL) within the Security Descriptor (SD) of the file or folder.

The ACL of a resource is exposed in the UI by the ACL Editor. The Windows Server 2003 ACL Editor is strikingly different from Windows NT 4.0. It has several *levels*, each accessible by command buttons. For example, if you right-click any NTFS file or folder, select Properties, then click the Security tab, you will see a general overview of the SD—what we call ACL 101—or the Security Settings dialog box. Click the Advanced button to see more detailed information—what we call Level 2—or the Advanced Security Settings dialog box. Select any permission and click View/Edit to see even more detail—what we call Level 3—or the Permission Entry dialog box.

Default Permissions

The default permissions on a file or folder on a Windows Server 2003 system are significantly different than in Windows 2000 or Windows NT 4.0, in which the default permission was Everyone: Allow (Full Control). Windows Server 2003's default permissions are inherited from the parent object: in the end, the root of the disk volume. The default permissions on a folder are:

- System: Allow (Full Control). The System account represents the local computer. Many native and third-party services use the System account, and we recommend that you allow the System account Full Control of files and folders on the computer's local disk volumes. Therefore, the best practice is not to modify this permission.
- Administrators: Allow (Full Control). The local Administrators account is allowed full control by default. The local Administrators account is able to access all resources on the system and, through a variety of mechanisms, change permissions and grant itself full control. Administrators can always gain full control of local resources; and preventing the local Administrators group from accessing local resources is not always possible. Therefore, unless you want to force Administrators to jump through the hoops required to take ownership, change permissions, and access a resource (each of which can be audited), allowing Administrators full control is customary.
- Creator Owner: Allow (Full Control). This permission has the effect that the user that creates a new file or folder gains full control of that file or folder. The Creator Owner special account is a placeholder on a container object. When a new child object is created, the permission assigned to Creator Owner is assigned to the object's creator.

- Users: Allow (Read and Execute). This permission allows members of the local Users group (which contains the Domain Users group by default) the ability to read files and folders.
- Users: Allow (Create File) and Users: Allow (Create Folder). This permission allows members of the local Users group to create new files and folders inside a folder. As we mentioned earlier, the user that *does* create a new file or folder gains full control of that object through the Creator Owner permission.

In summary, Administrators and the System have Full Control and Users have the ability to open and read files and folders. In addition, any user can create a new file or folder at which point that user has Full Control permission to that resource.

Configuring Permissions

You can use the ACL Editor to add, remove, or change permissions to a resource through accounts.

Add a Security Principal to the ACL

1. Right-click the resource and select Properties.
2. On the Security tab of the Properties sheet, select the account for which the permission is needed; or if the account name is not present, click the Add button, then select the security principal.
3. To select the appropriate permissions template, click the checkbox for the template.

For advanced permissions:

1. On the Security tab of the properties sheet, click the Advanced button.
2. To select the appropriate security principal or add the security principal to the list, use the Add button.
3. Select the checkbox next to the desired permissions settings.

Keep these tips in mind:

- Configure permissions only on groups (not users) and preferably domain local or universal groups (local groups in mixed mode).
- Click each account in the Names list and confirm all permissions in the Permissions list before clicking OK to finish.
- Watch for the item on the Security tab's permissions list labeled Special. This tab shows that there are permissions that do not comply to a standard permissions template. Click the Advanced button to see all permissions on the object.

Inheritance

ACLs, like several other Windows components, are characterized by inheritance. With ACL inheritance, you can configure permissions of a container, such as a folder, and those permissions will propagate automatically to that container's contents.

Note

When a folder is given a set of permissions, most of those permissions are *inheritable* and will be passed down to all the objects in that folder by default. This inheritance is because child objects are configured to *allow inheritable permissions from the parent to propagate to this object* by default.

An administrator needs to set permissions only once at the parent folder level, and those permissions will propagate to child objects.

Review these important notes regarding inheritance:

- Windows Server 2003 inheritance is granular and dynamic. If a child object is configured to *Allow inheritable permissions from the parent to propagate to this object*, then any changes to permissions on the parent container will automatically propagate to the child without any administrator intervention. Inherited permissions do not remove permissions assigned explicitly to the child object.
- Inheritance in Windows Server 2003 is very different from inheritance in Windows NT 4.0. Inheritance in Windows NT 4.0 was similar to the *Replace permission entries on all child objects* option in the Windows Server 2003 ACL Editor—it forced the permissions of a folder down the folder tree, removing all other permissions in the process.
- Inheritance is the combined effect of inheritable properties of a parent (Level 3 of the ACL Editor) and a child that allows inheritance (Level 2 of the ACL Editor).
- Managing with inheritance wherever possible, so that properties can be administered at a point high in the folder tree, is a best practice.
- Inheritance can be blocked for objects low in the tree and can be forced back down the tree from a parent.

Blocking Inheritance

However, in certain situations applying a different set of permissions to a child object than those applied to a parent folder is necessary. Then *blocking* inheritance or overriding inheritance with explicit permissions on the child object becomes necessary.

Tip

If you need to block inheritance or set explicit permissions too often, you should check whether or not your file management (your folder structure) needs modification.

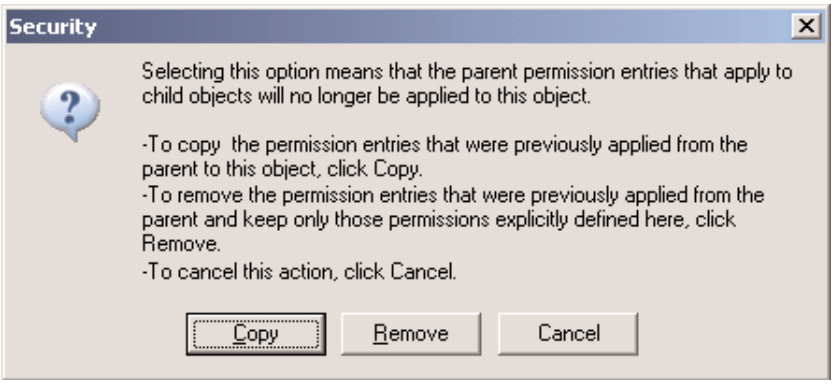
Block Inheritance

1. Right-click an object and select Properties.
2. Select the Security tab.
3. Click the Advanced button.
4. Clear the *Allow inheritable permissions from parent to propagate to this object* checkbox.

5. Choose to either Copy the parent's permissions explicitly to the resource's ACL or to Remove them entirely from the resource's ACL, as Figure 10 shows.

Figure 10:

Selecting Copy or Remove Permissions in a Security Dialog Box



The message that Figure 10 shows is the cause of much confusion on the part of new administrators of Windows Server 2003. In the end, the choice you make doesn't affect the results. You will end up with an ACL on the object that contains only explicit permissions—the object will no longer inherit the permissions of the parent object, and the explicit permissions assigned to the object will solely determine access to the object.

The Copy or Remove Permissions dialog box asks how you want to build the new ACL. To start with an empty ACL, select Remove, then you can add permissions that you desire on the ACL. Or you can choose Copy, in which case the new ACL is populated with explicit permissions that match the permissions that were previously inherited. Then you can remove the permissions you do not want to keep and add new permissions. So this dialog box lets you choose the easiest method for you to create the new ACL.

Tip

When deciding whether to copy or remove permission settings, choose the option that is closest to the explicit permission settings that you want to set on the object. For example, if you want essentially the same settings with just a few changes to a lengthy and complex ACL, then the best choice would be to Copy the permission settings and make the changes afterward.

6. Modify the permission settings as necessary.

Reinstating Inheritance

If reinstating inheritance to an object becomes necessary, you can use two methods to do so. Each produces different results.

Reinstate Inheritance on an Object

The first method is to reinstate inheritance on the child object.

1. Right-click the child object and select Properties.
2. Select the Security tab.
3. Select the *Allow inheritable permissions from parent to propagate to this object* checkbox.

Note

This action will result in the inheritable permissions from the parent folder becoming again inherited by the child object *with the existing explicit permissions of the child object remaining in force*.

Reset Permissions to Enforce Inheritance from a Parent Folder

The second method is to reinstate inheritance from the parent folder by resetting child permissions and enforcing inheritance.

1. Right-click the parent folder and select Properties.
2. Select the Security tab.
3. Click the Advanced button.
4. Select the *Reset permissions on all child objects and enable propagation of all inheritable permissions* checkbox.

Note

Note that this checkbox control acts like a command button: It applies the requested action one time; it does not enforce inheritance into the future. When you return to the dialog box, it will be cleared.

5. To confirm the selection click Yes.

Note

This option *removes all the explicit permissions* on the child objects. The ACLs on child objects will be clean with only the permissions inherited from the parent folder.

Effective Permissions

The effective permissions, which ultimately determine the level of access, are determined by the cumulative effect of allowed, denied, explicit, and inherited permissions. To understand how the effective permissions are derived, we must look at the hierarchy of permission settings and their precedence on an ACL.

Following are the golden rules of permission settings.

File Permissions Override Folder Permissions

The only ACL that matters is the ACL for the object that is being accessed. When a user has only Read permission on a folder and when Full Control permissions are given to a child object, such as a file, the user will have Full Control over that object. The same is true in reverse, so when the user has Full Control for a folder, but only Read permission on the file, the user can read but not modify the file.

Permission Settings

Permissions have five states:

- Not Specified (both Allow and Deny are cleared)
- Explicit Allow (Allow checkbox is checked)
- Inherited Allow (Allow checkbox is grey and checked—the permission is inherited from the parent folder)
- Explicit Deny (Deny checkbox is checked)
- Inherited Deny (Deny checkbox is grey and checked—the permission is inherited from the parent folder)

Implicit *No Access*

A setting that is *unspecified* has the effect of not allowing access because there is no specific permission setting. For example when a user is a member of eight groups, none of which is given an Allow permission to a resource, the user is denied access. However, if one group has an Allow permission, the user will have access at the level specified.

Allow Permissions Are Cumulative

Whether you assign permissions to a user or to a group or groups to which a user belongs, all the permissions apply to the user. For example, when a user is individually given Read permissions to a file and is a member of a group that has Write permissions, the user will have both Read and Write permissions. If that user is also a member of another group that has Full Control of the parent folder and inheritance is in use, then the user will have Full Control of the resource.

Deny Overrides Allow

A Deny permission takes precedence over an Allow permission, so even when a user is a member seven of groups that have Allow permissions to a resource specified, the user will be denied access if one group is assigned a Deny permission.

Explicit Permissions Override Inherited Permissions

A checked gray checkbox in the ACL editor indicates that permissions are being inherited from a parent folder or multiple parent folders. Although the default condition is that the permissions will be cumulative between inherited permissions and explicit permissions, indicated by a checked white checkbox, in the event the two should contradict, the explicit permission will override the inherited. For example, suppose a user has an inherited Deny Read permission, but a group to which that user belongs has an explicit Allow Read permission. The Allow permission will take precedence and the user will be able to read the file.

Evaluating Effective Permissions

Windows Server 2003's ACL Editor provides a handy way to evaluate what permission a user or group has for that object. Click the Advanced button on the Security tab of the object's Property dialog box. Then click the Effective Permissions tab. Select the user or group for which you want to evaluate effective permissions. Then the tab calculates permissions based on the rules described earlier.

Best Practices for ACLs

The following summarizes best practices for ACLs on files or folders:

- Assign the minimum permissions necessary for resource access.
- The default permissions are adequate for many scenarios in Windows Server 2003.
- The Full Control permission is usually appropriate only for administrators, the System account, the Creator Owner account, and the user or group that *owns* the resource.
- You should typically grant other accounts Read and Execute or Modify permission at most. The Modify permission provides read and write capability, but does not allow the user to change permissions on the object or delete the object. Full Control adds those two permissions plus the Delete Subfolders and Files permission.
- Unlike Windows 2000 and Windows NT 4.0, in Windows Server 2003 the Everyone group is restricted so that anonymous connections are not included. Therefore, the Everyone group can be used with more regularity on ACLs.
- Use a broad, shallow folder structure and aim to manage all permissions through inheritance.
- Do not use share permissions to restrict access. The correct share permission is Everyone (Full Control).

Sharing a Folder

After a folder has been appropriately secured, you can make it accessible to remote users by *sharing* the folder. The process of sharing a folder has not changed: right-click the folder, select Properties, click the Sharing tab (or select *Sharing and Security* from the shortcut menu), and select *Share this folder*.

However, the default permissions applied to a shared folder have changed. Windows Server 2003 sets the default share permission to Everyone (Allow Read). Although this default setting is technically more secure, it violates the best practice of securing a file or folder *only* with NTFS permissions. Because share permissions (which are more restrictive than NTFS permissions) will win, even administrators are prevented from modifying the contents of a shared folder.

Most enterprises have a written policy that specifies that shares should be configured with Everyone (Allow Full Control), then secured with NTFS permissions.

Tip

When configuring a shared folder, be sure to click the Share Permissions button and grant the Everyone group Full Control.

Other Guidance on What Is New

To help you maintain continuity of administration, the earlier sections of this chapter guide you through the most common day-to-day administrative tasks. A full discussion of administering Windows Server 2003 and Active Directory is beyond the scope of this eBook. For a comprehensive discussion of Windows Server 2003 administration, check out the eBook, "Windows 2003: Active Directory Administration Essentials," available at http://www.windowsitlibrary.com/Ebooks/AdministeringAd/Index.cfm.

The following sections will help you to identify other administrative features and concerns that might warrant additional attention.

Help and Support Center

The Windows Server 2003 online Help feature is extraordinary. The Help and Support Center (in the Start menu) centralizes tools and documentation. The Search functionality searches across the online Help documentation as well as the Microsoft Knowledge Base (when you have an Internet connection). And the online Help is extremely well written: comprehensive and easy to follow.

You can even install the Windows Server 2003 Help on a Windows XP client (and vice versa), which lets you easily access Help and support for both platforms.

Note

For more information about how to install Windows Server 2003 Help on a Windows XP system, see the Microsoft Web site at http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/sag_ATP_sharehelp.asp.

Microsoft IE Enhanced Security Configuration

The Internet Explorer (IE) Enhanced Security Configuration locks down IE on Windows Server 2003. This configuration prevents access to untrusted sites and in the end requires you to authorize each site you want to visit.

You can disable the configuration for all users on a server (for example, in a Terminal Services configuration) or just for administrators. Use the Add/Remove Programs application in Control Panel and select Add/Remove Windows Components. In the components list, select the IE Enhanced Security Configuration and click Details. You can specify whether the configuration should apply to administrators, nonadministrative users, or both.

Shadow Copies

The Shadow Copies feature lets administrators or users recover previous versions of files when the current version is corrupted, overwritten, or deleted. This feature is an easy and effective alternative to restoring the file from backup media and can be implemented in conjunction with a complete backup plan. To enable shadow copies, right-click a volume on a Windows Server 2003 computer and click the Shadow Copies tab. Then click the Enable button.

To use the shadow copies functionality to recover a file, you must use a Universal Naming Convention (UNC), for example *servername**sharename*), to access the appropriate folder, then

right-click the folder or file, choose Properties, and click the Previous Versions tab. This interface—the Previous Versions client—is native to Windows Server 2003 computers but can be installed on Windows XP and Windows 2000 systems.

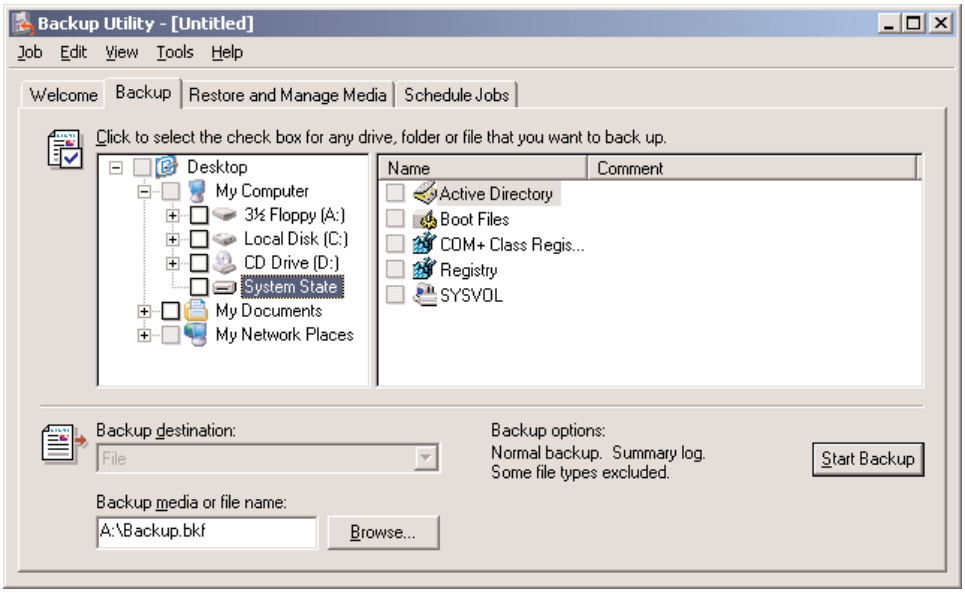
The Shadow Copies feature has many possible configurations and nuances. Use the Help and Support Center documentation to learn the ins and outs of Shadow Copies.

Disaster Planning and Recovery

Including Active Directory in your disaster recovery planning is important. To back up Active Directory, back up the System State of a DC. The System State is a collection of components, including Active Directory, the Sysvol, the registry, and other items that drive the configuration of the server. You cannot back up an individual element of the System State: the System State is backed up as an entirety. Using a backup utility, such as the builtin Backup Utility (ntbackup.exe), select the System State node, which Figure 11 shows.

Figure11:

Displaying the System State in the Backup Utility Dialog Box



To restore Active Directory on a failed DC, you must restart the DC and press F8 when prompted. A series of startup options will appear including the Directory Services Restore Mode. Select this mode and the DC will start without directory services being active—it is a kind of *safe mode* for directory services. Because directory services is not running, related files are not locked and can therefore be restored from the backup media. Using the backup utility of choice, restore the System State onto the DC.

After the restore operation has completed, restart the DC in the normal manner. The DC will initiate replication from its partners to get *up to date*, because its directory database will be accurate as of the date of the System State backup.

Active Directory backup and recovery has many nuances. Be certain to read the information in the Help and Support Center.

Monitoring DC Health

A few tools are available in the native administrative tools to monitor DC health. Monitoring DC health is important, unless you are comfortable with the *firealarm* monitoring methodology in which you find out something has broken only when it causes enough pain that people notice.

Among the important components of Active Directory that you should monitor are:

- **DNS records**. Periodically query the DNS zone to ensure all required service and host records are registered so that clients can locate all DCs and services.
- **DC accessibility**. Perform tests such as simple as pings to appropriate ports to check whether DCs can be accessed across the network.
- **Replication**. Replication is a complex process that works amazingly well with little intervention in most enterprises. But when it breaks, it is painful. Replication checks will report any problems with replication, and with any luck, before replication problems cause pain.
- **Trust relationships**. Validate trust relationships with external domains.

Third-Party Administrative Tools

The native administrative tools support basic administrative tasks in simple environments. If your enterprise is more complex (with multiple domains, multiple forests, or multiple directory services), you might require tools that create virtual views of the organization to let you manage the environment more flexibly. Native administrative tools are also weak in the areas of monitoring and reporting.

NetIQ, the sponsor of this eBook, offers several products that enhance your ability to monitor, manage, and troubleshoot Active Directory and Windows Server 2003. NetPro specializes in monitoring Active Directory, and information about its tools is available at http://www.netpro.com. Chapter 4 provides a list of other companies that offer administrative tool suites that you might want to evaluate.

Next Steps

Windows Server 2003 and Active Directory provide a stable, secure, scalable platform on which to deploy enterprise services. In the next chapters, we focus on what has become an indispensable enterprise application: email. We will migrate older versions of Microsoft Exchange Server to Exchange Server 2003, and you will find that tools such as the Active Directory Migration Tool will again serve an indispensable role.