

ITProTM
SERIES

Windows
A NET MAGAZINE

 **eBooks**

Windows 2003: Active Directory Administration Essentials

By Jeremy Moskowitz



net iQ

mission critical software for e-business



Contents

Chapter 3 What's New in Windows 2003 Active Directory Management	43
New Administration Console Features	43
Drag-and-Drop Function	44
Multiple Select Function	45
Saved Queries Function	46
Group Policy Management Console	48
Installation and Initial Use	49
GPMC Basic Use	50
the GPMC's New Functions	50
New Forest Options	51
Defining the Problem	51
Win2K's Solution	54
Windows 2003's Solution	54
What a Federation Does and Doesn't Offer	55
Creating Cross-Forest Trusts	56
Next: Delegation and Security in Windows 2003	62

Chapter 3:

What's New in Windows 2003 Active Directory Management

In Chapter 2, I discussed the ins and outs of the compatibilities between Windows NT 4.0, Windows 2000, and Windows Server 2003 (Windows 2003). I explored several domain modes in both Win2K and Windows 2003 and several forest levels in Windows 2003. In this chapter, I review some of Windows 2003's key new features, including the additional functionality in the Active Directory Users and Computers console, the Group Policy Management Console (GPMC), and the ability to set up forest trusts. Some features don't require Windows 2003's domain functional level or Windows 2003's forest functional level; others do. I point out where and when you can use specific features.

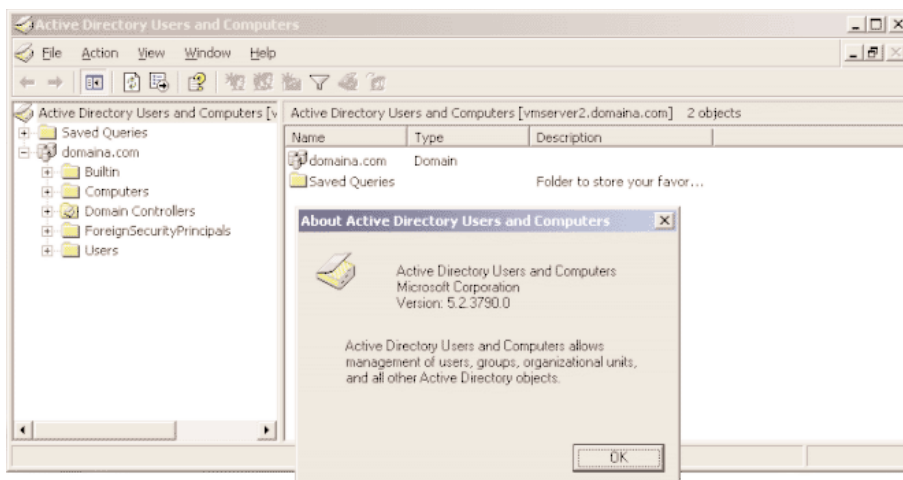
New Administration Console Features

As soon as you load your first Windows 2003 domain controller (DC), you're armed with the latest set of administration tools. In Win2K, the key management tool for Active Directory (AD) has been the Active Directory Users and Computers console. Updated with several useful features, the console remains your main tool.

You can ensure you're running the Windows 2003 version of the Active Directory Users and Computers by using Help, About. The About Active Directory Users and Computers dialog box should display version is 5.2.x, as Figure 3.1 shows. (The version will probably change as Microsoft introduces Windows 2003 service packs.)

Figure 3.1

Checking the Active Directory Users and Computers version

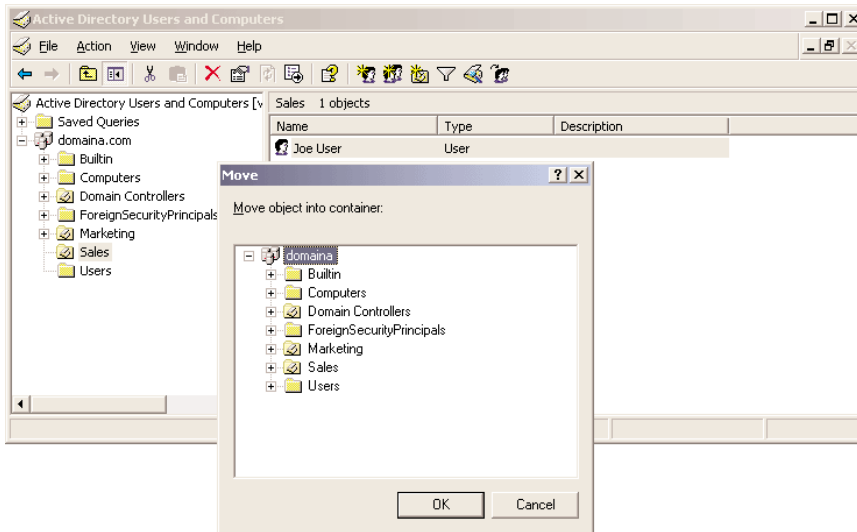


Drag-and-Drop Function

One of the most requested features for this version of Windows was a drag-and-drop function within Active Directory Users and Computers. In Win2K's version of the Active Directory Users and Computers tool, you could move objects around the AD only by right-clicking them, selecting Move, and selecting the destination. This option is still available in Windows 2003, as Figure 3.2 shows.

Figure 3.2

Moving objects through Active Directory Users and Computers



However, with Windows 2003, you now have the requested additional option. You can simply drag a user account or multiple user accounts from one folder or organizational unit (OU) to another folder or OU.



Note

In Windows 2003's Active Directory Users and Computers, you can still move items by right-clicking and selecting Move rather than by using the new drag-and-drop feature.



Tip

I continue to use the Win2K-style method of right-clicking and moving the objects rather than dragging them. I fear moving an entire group of users or an OU from one corner of AD to another inadvertently. Continuing to right-click and move my items is a bit slower, but doing so reassures me that I've made a deliberate move.

Multiple Select Function

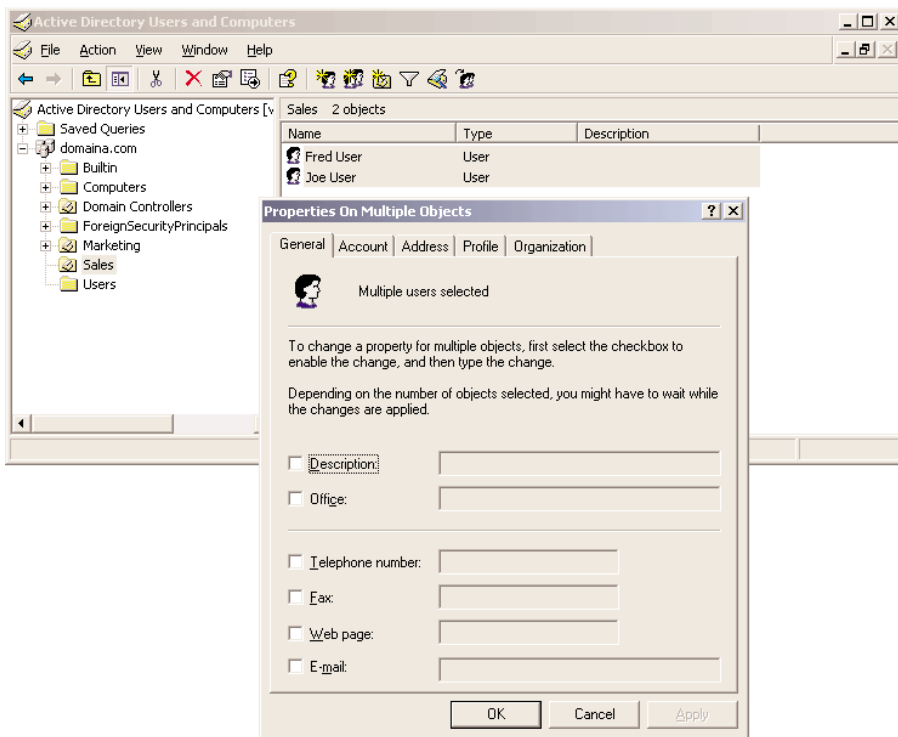
The next-most-requested feature for Windows 2003 also involves the Active Directory Users and Computers console. That is, the ability to select multiple items within Active Directory Users and Computers (e.g., 10 users) and change some element of all the items' information (e.g., changing all the users' business addresses to a different location).

To make such a change in AD previously, you had to either individually plunk the information into each user's account or write an AD-enabled script, such as a Visual Basic (VB) script, to zip through each account you wanted to change and add the data. Neither approach was appealing. Active Directory Users and Computers' new functionality makes some formerly difficult tasks, including this one, easy.

To try this feature, simply hold down the shift key and select multiple accounts, right-click after you've selected the last account, and select Properties. You'll then see a special Properties On Multiple Objects dialog box, which Figure 3.3 shows.

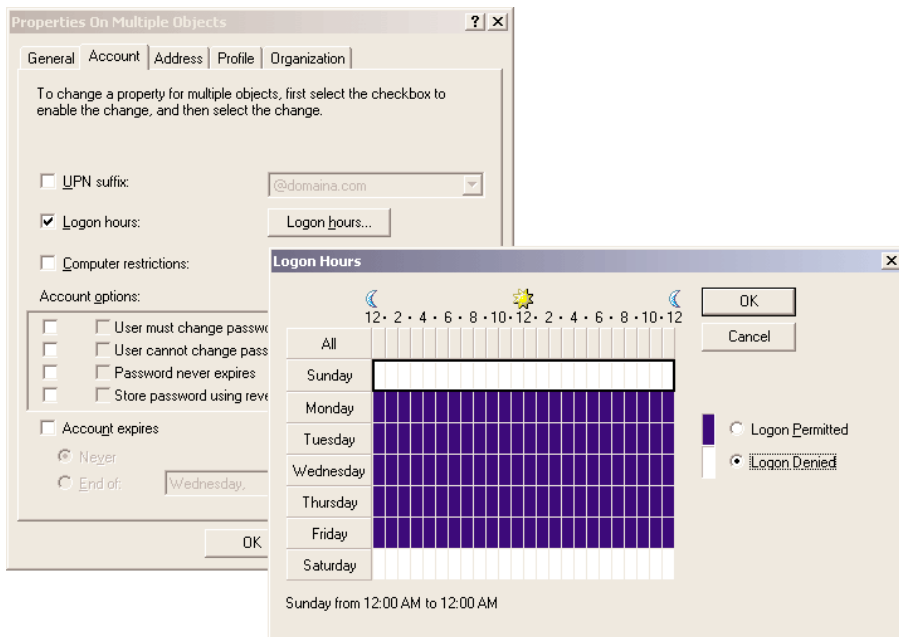
Figure 3.3

Selecting multiple users in Active Directory Users and Computers



As Figure 3.3 shows, the Properties On Multiple Objects dialog box reminds you that you have multiple users selected. You click the tab that contains the information you want to change, then select the check box for the information you're modifying (e.g., address, account expiration date). Figure 3.4 shows the available tabs and the Logon Hours dialog box that appears if you select to change users' logon hours.

Figure 3.4
Changing properties for multiple objects at once



When you click OK, you leave intact all the current information each account contains but replace the information you entered after selecting the appropriate check box. The new multiple-select capability of Active Directory Users and Computers is a great time-saver.

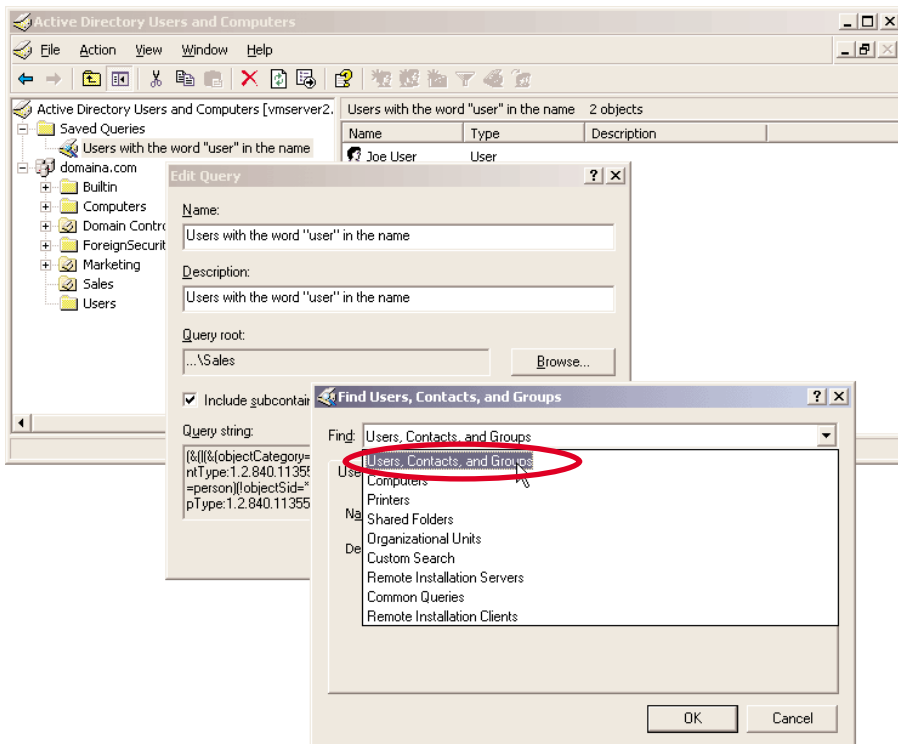
Saved Queries Function

One common problem with Win2K's Active Directory Users and Computers has been that the console wasn't meant to perform repetitive tasks. For example, you might want to locate all users who met certain criteria within a specific OU or across the entire domain. In Win2K, if you wanted to locate all users whose accounts were in the Sales OU who hadn't logged on in the past 30 days, for example, you faced a difficult task. Typically, you'd have to hand-craft an Active Directory Service Interfaces (ADSI) script through VBScript to perform this search. Windows 2003's Active Directory Users and Computers makes short work of this once-tedious task with a new feature called Saved Queries.

For this example, let's find everyone in the Sales OU with "user" in his or her name. You can create and save new queries by right-clicking the Saved Queries folder and selecting New, then Query. Name your query and begin to select the criteria for your search by clicking Define Query.

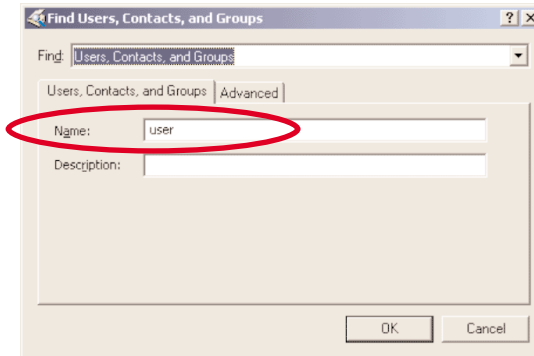
Locate and select the category of AD object category for your search, such as Users or Printers. Figure 3.5 shows how you create a custom search.

Figure 3.5
Search options for locating objects in AD



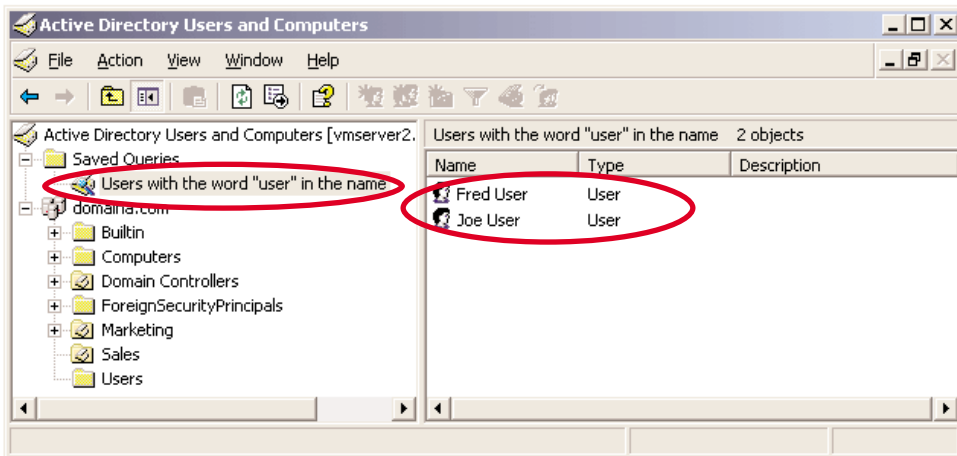
When you find the category you want to search, select it, and fill in the matching criteria. Figure 3.6 displays the query to find all users with the word "user" in the name field.

Figure 3.6
Query to find users with the word “user” in the name



When the search has completed, you can immediately access the results. Figure 3.7 shows the list of users with the word “user” in the name field.

Figure 3.7
Displayed results of a saved query



You’ll find the ability to create and save new queries useful. With this feature, Windows 2003’s Active Directory Users and Computers has taken a practical step forward.

Group Policy Management Console

In addition to the enhanced Active Directory Users and Computers console, another major management advancement comes as a free download from Microsoft. The GPMC is an add-on for Windows 2003 and Windows XP Professional. The GPMC’s goal is to provide an enhanced view of and better management features for Group Policy.

**Note**

You can download the GPMC from Microsoft at

<http://www.microsoft.com/downloads/details.aspx?familyid=f39e9d60-7e41-4947-82f5-3330f37adfeb&displaylang=en>

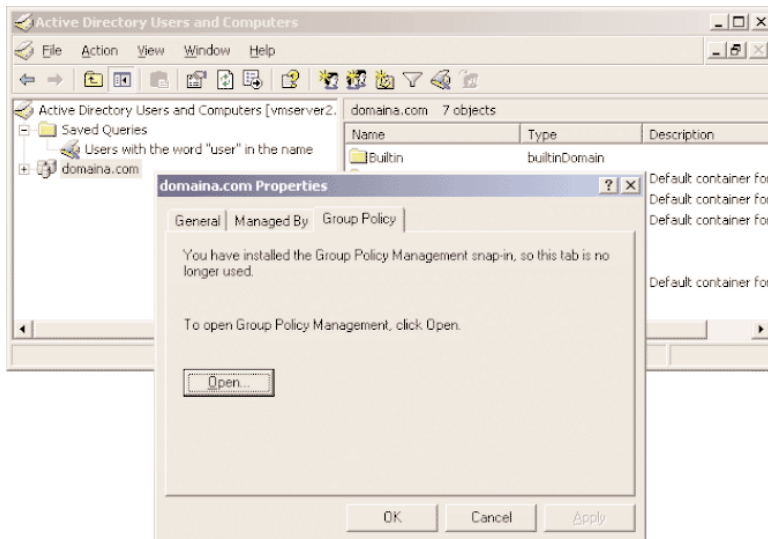
In Win2K (and in Windows 2003 without the GPMC loaded), you need to know where each Group Policy is maintained in relation to each domain and OU and sometimes in relation to each AD site. The complexity of what you need to know can make managing Group Policy confusing. The GPMC strives to provide a “Group Policy-centric” view of the environment – a bird’s-eye view of Group Policy Objects (GPOs).

Installation and Initial Use

Installation is pretty routine. Simply download the Windows Installer (.msi) file from Microsoft and place it where you want to perform your Group Policy management. For this example, I’ve loaded it on my Windows 2003 server.

After you’ve loaded the GPMC, you can start the console a couple of ways. Loading the GPMC effectively disables the former way of manipulating Group Policy. If you attempt to manipulate GPOs in the usual Win2K fashion, a dialog box offers you only one choice – to click Open and launch the console, as Figure 3.8 shows.

Figure 3.8
Manipulating GPOs after the GPMC is loaded



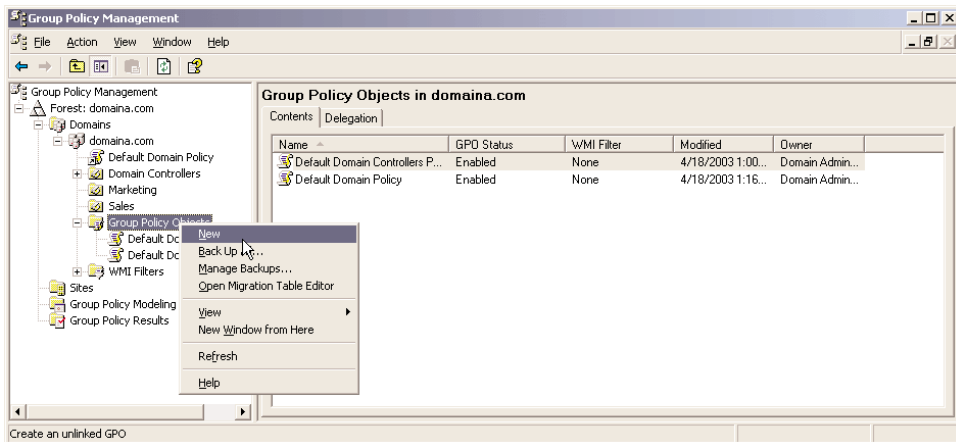
Alternatively, you can use an icon to launch the GPMC. An icon titled Group Policy Management appears automatically when you select Start, Programs, Administrative Tools.

GPMC Basic Use

One benefit of the GPMC is that you can see all your GPOs at once. Simply expand the tree to find your forests, domains, and OUs. You'll also see a special folder called Group Policy Objects, which Figure 3.9 shows.

Figure 3.9

The GPMC's Group Policy-centric view



You create new GPOs through the GPMC. After you create a GPO, you can edit it by right-clicking it and selecting Edit. Doing so launches the Group Policy Editor, which you can then use to set the policies you want to implement.

The GPMC's New Functions

You might be asking yourself why you would want to switch to another tool to do things you already accomplish another way. The GPMC brings a lot more functionality than you'll find in the base Windows 2003 product. The new GPMC features you should explore and evaluate include

- backup and recovery of GPOs. This much-needed feature simplifies what was previously a highly laborious task.
- increased reporting. Now you can get HTML-based reports that show the settings inside a GPO.
- “Resultant Set of Policy” modeling. This modeling feature lets you determine what policies a user will be assigned if he or she moves, for example, from one OU to another OU. This modeling capability works only if you're connected to a Windows 2003 DC in the domain in which you're trying to perform the modeling.

The GPMC is packed with features that you won't want to miss. I can't review every feature, so be sure to download the GPMC and see what it has to offer. I think you'll be pleasantly surprised.

**Note**

I'll fully explore the GPMC in the upcoming revision of *Windows 2000: Group Policy, Profiles and IntelliMirror* titled *Windows Server: Group Policy, Profiles and IntelliMirror*. For information about the current edition and about the revision as soon as it's available, go to <http://www.sybex.com/sybexbooks.nsf/2604971535a28b098825693d0053081b/d15f21a26eaeed8588256bca0062a12f!OpenDocument&Highlight=0,moskowitz>

New Forest Options

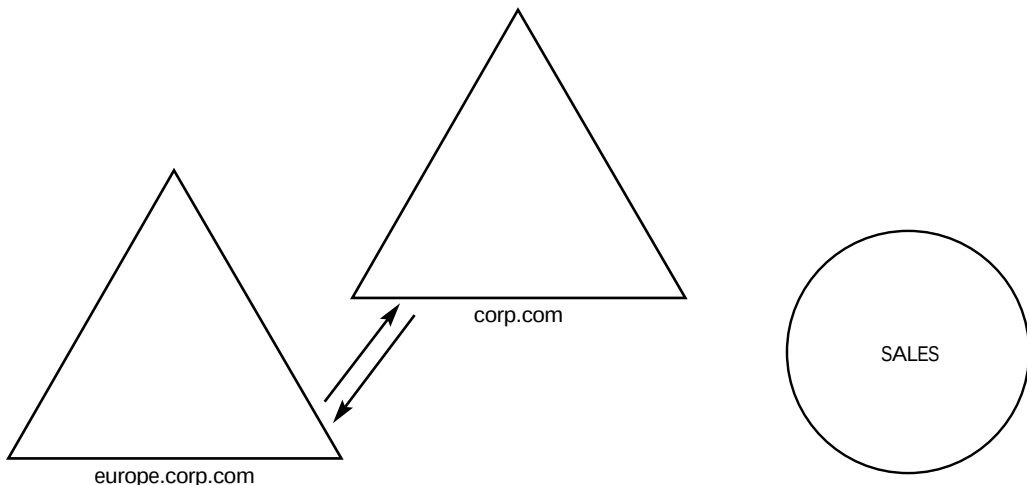
Win2K has been missing something that our friends in the Novell world have: the ability to prune and graft portions of the directory service. Although Windows 2003 doesn't introduce pruning and grafting, it does offer one new "patch" that solves part of the problem.

Defining the Problem

In Win2K, you could upgrade an NT 4.0 domain into a current Win2K forest. For example, if you had already established your Win2K forest and wanted to add an NT 4.0 domain, it was quite easy. Take the example of the Corp.com Win2K tree and the currently "uninvolved" NT 4.0 Sales domain, which Figure 3.10 shows.

Figure 3.10

An NT 4.0 domain not yet in an existing Win2K domain



You can upgrade the Sales PDC, instruct it to join an existing forest, and simply choose which domain you want to be the parent. Figure 3.11 and Figure 3.12 show possible upgrade options. Figure 3.11 shows the Sales domain becoming Sales.corp.com, a child of Corp.com.

Figure 3.11

Option 1 – Sales becomes Sales.corp.com, a child of Corp.com

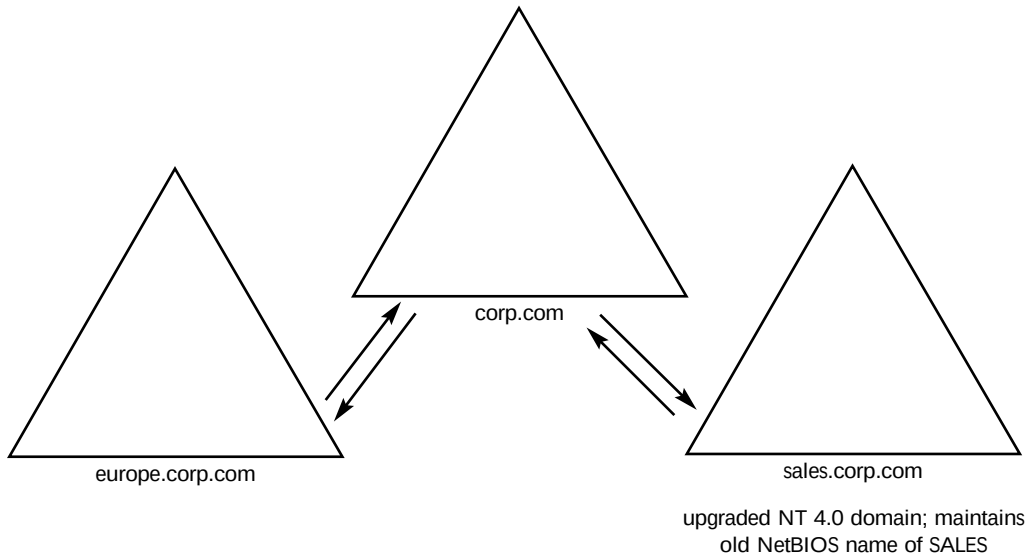
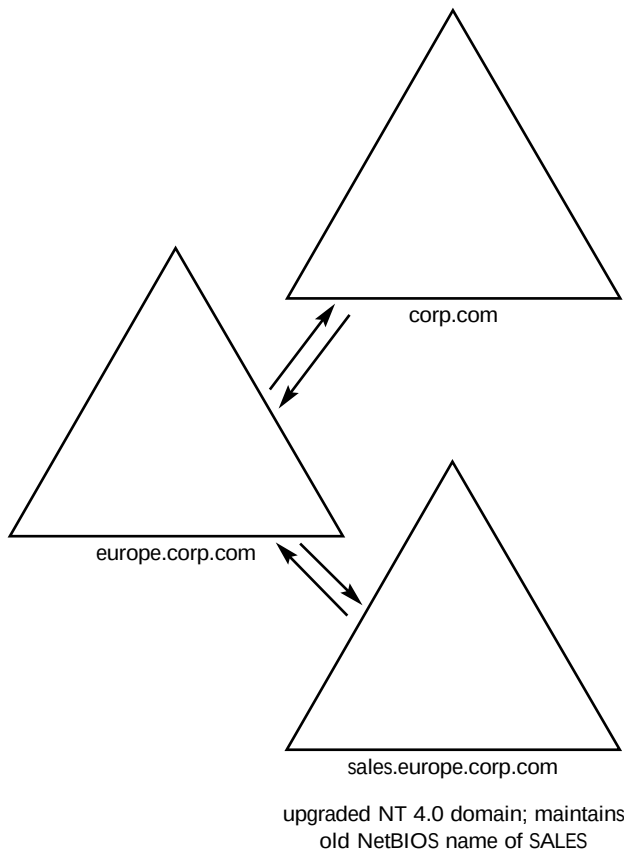


Figure 3.12 shows another upgrade option for the NT 4.0 Sales domain. The Sales domain becomes Sales.europe.corp.com, a child of the Europe.corp.com domain.

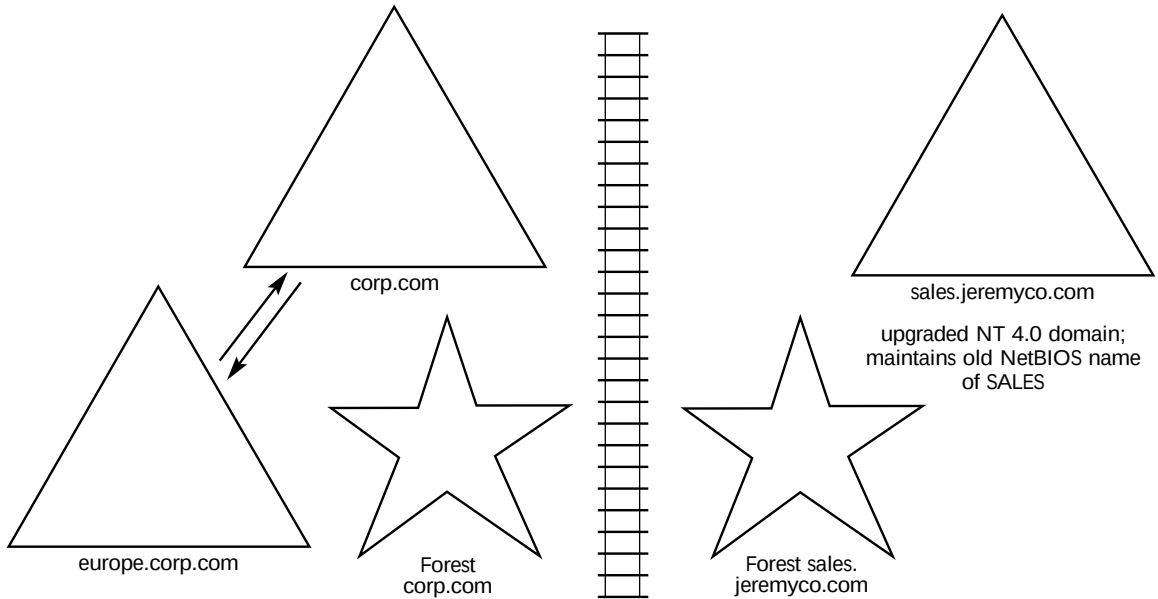
Figure 3.12

Option 2 – Sales becomes Sales.europe.corp.com, a child of Europe.corp.com



These two NT 4.0 domain upgrade options are useful, but they go only so far. Specifically, what happens if you already have two Win2K domain trees and no longer have any NT 4.0 domains? Such a scenario is quite prevalent in many corporations (e.g., when a merger has occurred). Someone has already performed the NT 4.0-to-Win2K upgrade in a domain – without choosing a Win2K parent. Later, an administrator wants to place that upgraded (now Win2K) domain (or domain tree) in an existing forest. In Win2K, you can't just "join" two existing Win2K domains or domain trees together.

Let's look again at the diagram in Figure 3.10. Imagine that the NT 4.0 Sales domain has been upgraded to Win2K without a parent domain having been chosen. The resulting situation would resemble the scenario that Figure 3.13 represents.

Figure 3.13*Two Win2K domains that can't simply be "joined"***Win2K's Solution**

The Win2K method for working around the inability to prune and graft isn't pretty. You set up external trust relationships between the unrelated domains. The external trusts work exactly like NT 4.0 trusts. However, like NT 4.0 trusts, the mechanism uses NT LAN Manager (NTLM) authentication, which means the connection isn't very secure. Additionally, every time you want a new domain in either forest to be able to share information with other domains, you must create another trust relationship manually.

An external trust lets you share basic account information through the trust – in the same way that NT 4.0 domains let you share such information. For example, after an external trust is put in place, you can apply NTFS permissions in one domain that also restrict users from another domain.

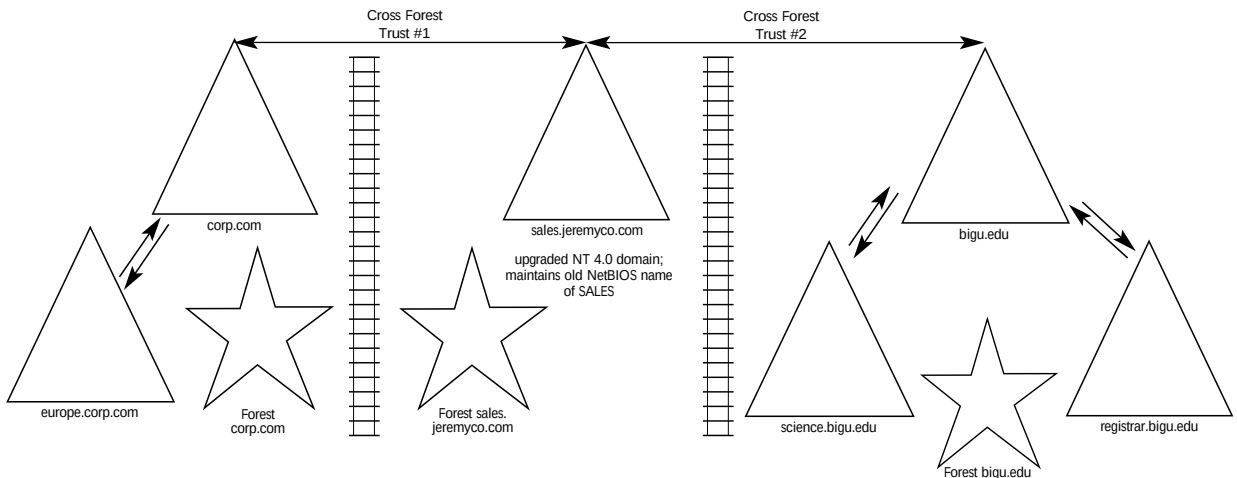
Windows 2003's Solution

Windows 2003 brings a new concept to the table: forest trusts. Cross-forest trusts let you loosely tie together two (or more) unrelated forests. You "tie" the forests together at each forest's root domain. Figure 3.14 shows an example of three unrelated forests tied together with cross-forest trusts.

**Note**

In Windows 2003, forests have names just as domains have names. The forest has the same name as the root of the domain of that forest, as Figure 3.14 shows.

Figure 3.14
Cross-forest trusts



When you tie multiple forests together with cross-forest trusts, the resulting set of relationships has a special name. It's called a "federation" of forests.

What a Federation Does and Doesn't Offer

Cross-forest trusts bring something to the table that Win2K external trusts can't offer: Kerberos-based authentication between forests. Because the trust is 100 percent Kerberos-based, it can leverage how AD works – in ways that NT 4.0 could not.

With the ability to leverage AD, administrators and users get some big benefits. Administrators no longer need to worry about manually creating a new trust between established domains and a new domain – should a new domain pop up. Because the new domain is automatically trusted, no new trusts are necessary.

Users also get a benefit – that is, they can log on from any domain in any forest. However, users must know their user principal name (UPN) to log on if they travel to any domain located "beneath" one of the roots, as the following examples demonstrate. If Fred from Corp.com traveled to the Domain sales.jeremyco.com, he should be able to see Corp.com in the drop-down box. This option is available because Fred is logging on from a domain that's one of the root domains.

However, if a user in Registrar.bigu.edu traveled to Europe and wanted to log in at a machine in Europe.corp.com, he would have to use his UPN logon name, joe@registrar.bigu.edu, to log on successfully. He couldn't use his usual method of picking his home domain from the Ctrl+Alt+Del drop-down box when he logged on. It simply doesn't appear. Therefore, I recommend that users become familiar with their UPN logon names – so they can log on from wherever they are.



Caution

Training your users to use the UPN-style logon could be an uphill battle if they're used to the ease of a drop-down box.

Administrators face a similar situation. That is, if administrators want to set ACL permissions on users across the cross-forest trust, the administrators must know the full UPN name of any accounts they want to manipulate. This shortcoming could make cross-forest trusts a bit annoying.



Note

To learn more about UPN logon names, go to <http://support.microsoft.com/default.aspx?scid=kb;EN-US;243280> or to <http://www.winnetmag.com/WindowsServer2003/Index.cfm?ArticleID=38280>.

Creating Cross-Forest Trusts

To create cross-forest trusts (and then a federation of forests), you must first make sure that the forests are at Windows 2003's forest functional level. As you recall, Windows 2003's forest functional level means that

- you have no NT 4.0 or Win2K DCs
- you've "pulled the switch" in each domain to ensure that it's in Windows 2003's domain functional mode
- you've also "pulled the switch" in the forest to ensure that it's at Windows 2003's forest functional level

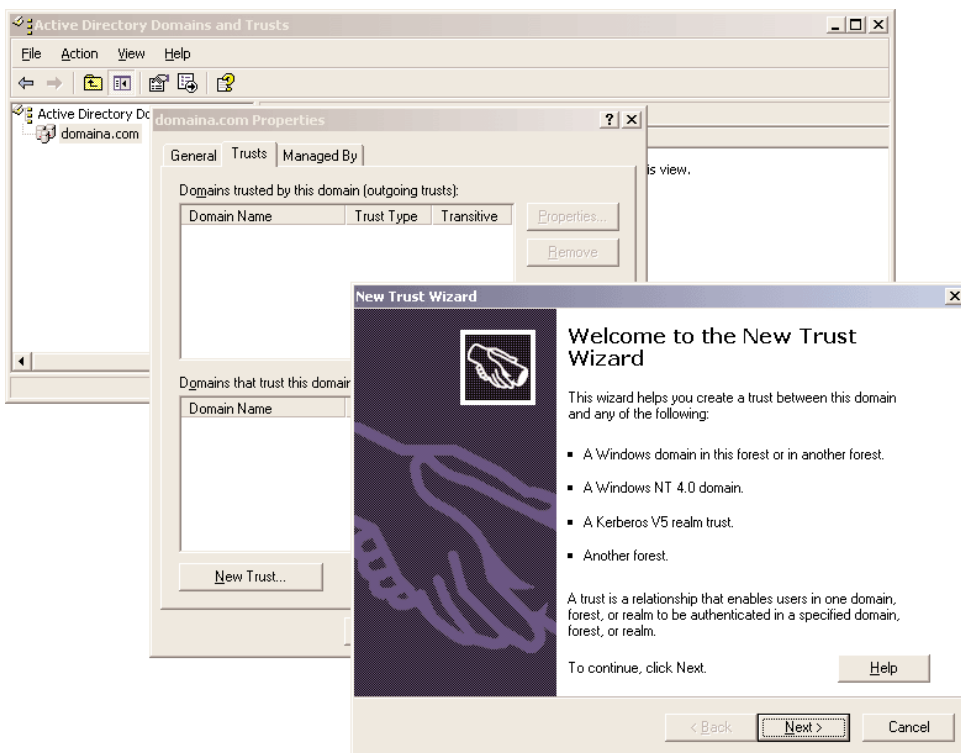
If every forest that you want to federate is at Windows 2003's forest functional level, you're ready to continue. In the following example, I create a cross-forest trust between a forest that contains Domaina.com and a forest that contains Corp.Com.

**Tip**

You can perform the work from whichever domain you choose, as long as it's from the root of one of the forests.

Begin by running Active Directory Domains and Trusts. Then, for the domain from which you're working, select the domain's Properties, click the Trusts tab, and select New Trust. Selecting New Trust launches the New Trust Wizard, as Figure 3.15 shows. You use the New Trust Wizard to create all sorts of trusts, including cross-forest trusts.

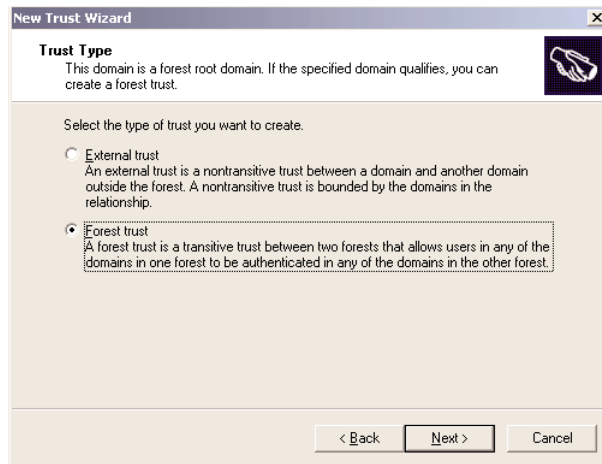
Figure 3.15
The New Trust Wizard



You can now design your cross-forest trust, which you can set up as a one-way or two-way trust. Be prepared for multiple wizard pages. Although I won't explore all of the pages here, I'll review highlights and examine the results of some choices you make.

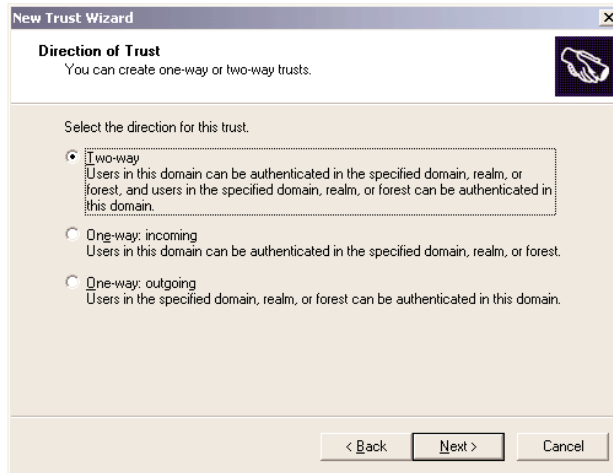
After the splash screen, the wizard displays the Trust Type page, which Figure 3.16 shows. You can select to set up a traditional NTLM External trust or a Kerberos Forest trust (i.e., a cross-forest trust). If you choose the NTLM External trust, the work you do here will be between just two specific domains and won't span the entirety of forests. It will be precisely the same as an NT-style trust, and you won't have any trust transitivity. (Kerberos supports transitive trusts. That is, if Domain A trusts Domain B and Domain B trusts Domain C, Domain A trusts Domain C.)

Figure 3.16
Selecting trust type



Next, the wizard displays the Direction of Trust screen, which Figure 3.17 shows. As its title indicates, on this screen you select the direction of the trust. The trust can be inbound to your forest or inbound to the other forest – or the trust can work both ways. You might choose to make the trust one way to share resources in one direction only. For example, you might have file servers in Forest A that Forest B must be able to access. However, Forest B might not need access to file servers in Forest A. In those circumstances, a one-way cross-forest trust might be just the ticket. Typically, however, you'll be setting up two-way cross-forest trusts.

Figure 3.17
Selecting trust direction

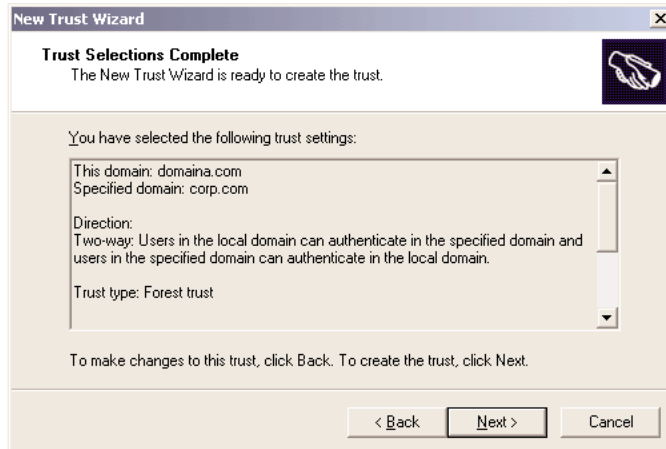


I omit the next screen, Sides of Trust, which lets you create both sides of the trust in one step. That is, instead of creating one half of the trust, then having the administrator of the other forest create the other side of the trust, you can simply give the system the other forest's credentials (if you have them) and create both sides of the trust at once. This creation option is a handy timesaver, as long as you have the administrative information you need.

The wizard then displays the Outgoing Trust Authentication Level – Specified Forest screen, which lets you determine which user accounts can go through the trust. I discuss this selection option, called the Authentication Firewall, in Chapter 4: Inside Windows Server 2003 Forests and DNS.

Finally, the wizard displays a summary of your selections on the Trust Selections Complete screen, which Figure 3.18 shows. On this example screen, you can see that I'm setting up a cross-forest trust between two root domains: Domaina.com and Corp.com.

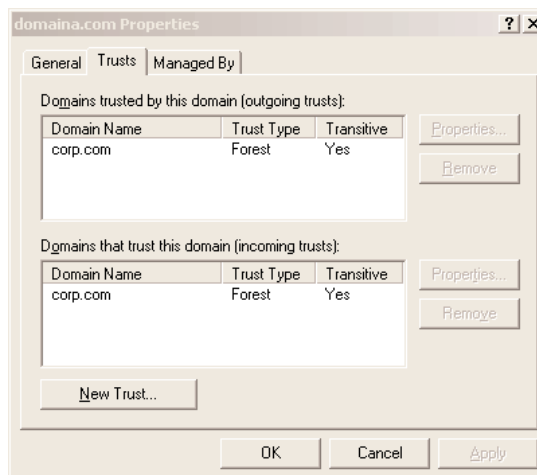
Figure 3.18
Trust Selections Complete summary screen



After the trust has been set up, Windows 2003 can automatically validate it. You choose the validation step on the screen that appears after you click Next on the screen that Figure 3.18 shows. The validation takes only a minute, and it ensures that after the initial trust is set up, it's valid and working properly from both forests. (Occasionally, one side of the trust can be built without the other side being built properly. This step ensures that the trust works correctly both ways.)

After you've finished setting up your trust, you can see the fruits of your labor inside Active Directory Domains and Trusts on the Properties screen, which Figure 3.19 shows.

Figure 3.19
The new cross-forest trust's properties



Because you're looking at Domaina.com's properties, you can see an inbound and outbound cross-forest trust to Corp.com.

Administrators in either forest can now choose accounts in the other forest and set permissions granting or restricting access to resources on the servers each "owns." Additionally, users can log on to any forest. Again, users can use the drop-down menu when they log on to any root domain, as Figure 3.20 shows. (You can see the other root domains from your domain and vice versa.)

Figure 3.20
Drop-down logon menu



Note

You can see both root domains listed in the drop-down menu. However, what you see isn't the Fully Qualified Domain Name (FQDN), such as Corp.com. You'll see only Domaina.com's and Corp.com's NetBIOS names – that is, DOMAINA and DOMAINC respectively. This can be tricky if users are expecting to find the FQDN name for logon purposes.



Caution

If users want to log on to computers in domains below any of the root domains (outside of their own forest), they'll have to know their UPN name, such as john@child-domain1.com.

I want to add a brief caveat regarding Windows 2003 and cross-forest trusts. The cross-forest trust goes a long way to "tie together" existing Windows 2003 forests. However, forest trusts don't tie together the GCs of disparate forests. Today, you simply have no way to magically tie the GCs together – and this limitation is bad news for those of you who use Exchange 2000 or who plan to use the upcoming Exchange 2003. Because the GCs aren't tied together, Exchange has no unified Global Account List. Essentially, you must still manage each forest's Exchange independently.



Note

Microsoft Identity Integration Server 2003 (formerly Metadirectory Services) is an up-and-coming way to put some magic back into managing Exchange across different forests. Microsoft Identity Integration Server 2003 looks promising.

Forests, then, are basically still separate, but cross-forest trusts between their roots make them federations that can share data and other resources.

Next: Delegation and Security in Windows 2003

Although Win2K is truly leaps and bounds beyond NT 4.0, Win2K has some deficiencies that Windows 2003 addresses. I've discussed three advantages that you gain with Windows 2003:

- updates to Active Directory Users and Computers that make AD easier to manage
- the new GPMC
- cross-forest trusts

In Chapter 4, I'll pick up where I'm leaving off. I'll explore how you can determine who can use the new cross-forest trusts – and more.