

ITProTM
SERIES

Windows
& NET MAGAZINE

 **eBooks**

Windows 2003: Active Directory Administration Essentials

By Jeremy Moskowitz



net iQ

mission critical software for e-business



Contents

Chapter 2 What's New in Windows Server 2003 Active Directory	23
Introduction	23
Working with Domain Levels	24
Analyzing Your Current Network	24
If You Have Combined Win2K and NT 4.0 BDCs	24
If You Have All Win2K DCs	28
If You Have All NT 4.0 Domain Controllers	29
Decision Point	30
Getting to Interim Mode	30
Sidebar: Why Does Interim Mode Exist?	30
If You Have No Windows-based Domains	32
Domain Level Review	34
Domain Functional Level Diagram	35
Working with Forest Levels	37
Windows 2003 Forest Functional Level Features	38
Preparing for the Upgrade	39
Using Adprep	39
Running Adprep /forestprep	40
Running Adprep /domainprep	42
Next: Window 2003 AD Management	42

Chapter 2:

What's New in Windows Server 2003 Active Directory

Introduction

“Chapter 1: Windows Server 2003 – What's New” introduced some of the many compelling features Windows Server 2003 (Windows 2003) brings to the table. Windows 2003 includes

- a faster, more secure, and re-architected Microsoft Internet Information Services (IIS) 6.0
- remote access quarantine through the Network Access Quarantine Control feature
- server event tracking through Shutdown Event Tracker
- greater scalability with more processors
- greater scalability with more cluster nodes

You can make a strong case for upgrading to Windows 2003 based on those features alone. If you simply walked around with the Windows 2003 CD-ROM and upgraded all your Windows 2000 member servers, you would have a field day exploring what you can accomplish with the new features. Of course, you won't want to walk around with the CD-ROM and perform those upgrades (you'd be likely to get into trouble). Nevertheless, Figure 2.1 shows the first screen you'll encounter when the time to upgrade comes.

Figure 2.1

Windows 2003 CD-ROM initial screen



In my opinion, the real magic of Windows 2003 lies in the new Active Directory (AD)-specific features you gain after you complete your upgrade. This chapter explores what capabilities those features provide and discusses how to prepare to use them.

Working with Domain Levels

To prepare for Windows 2003 AD, you must first ask yourself two questions: Which kinds of domain controllers (DCs) do I have and which kinds of DCs do I want to deploy? The answers to these questions might include Windows NT 4.0 BDCs, Win2K DCs, and Windows 2003 DCs. You'll want to begin by stepping back and analyzing your current network configurations.

Analyzing Your Current Network

Your network might contain

- all NT 4.0 DCs
- some Win2K DCs and some NT 4.0 BDCs
- all Win2K DCs
- no Windows-based domains (i.e., no network or a non-Windows network such as Banyan or Novell)

Each of these situations gives rise to some specific opportunities and concerns. I explore each scenario in the following text.



Note

Although it makes sense to list the scenario of having all NT 4.0 DCs first (as I did above), I discuss that scenario last. Moving from all NT 4.0 DCs to Windows 2003 has some unique considerations. Nevertheless, those of you who have all NT 4.0 DCs will benefit from reading through the material that precedes the discussion of that particular upgrade.

If You Have Combined Win2K and NT 4.0 BDCs

If you started out with NT 4.0 DCs and introduced a Win2K DC or two, you might remember the process. You had to begin with an NT 4.0 PDC and upgrade it directly into your Win2K Server. You probably made a backup of the PDC, then slipped in the Win2K CD-ROM with your fingers crossed. For 99 percent of the users who approached the upgrade this way, everything went well. For the other 1 percent of the users, the process involved sweaty palms as they rolled back the upgrade and tried to figure out what the problem was. After you completed the PDC upgrade, you had your first Win2K DC. In addition, Win2K advantageously put you directly into what's called Mixed Mode.

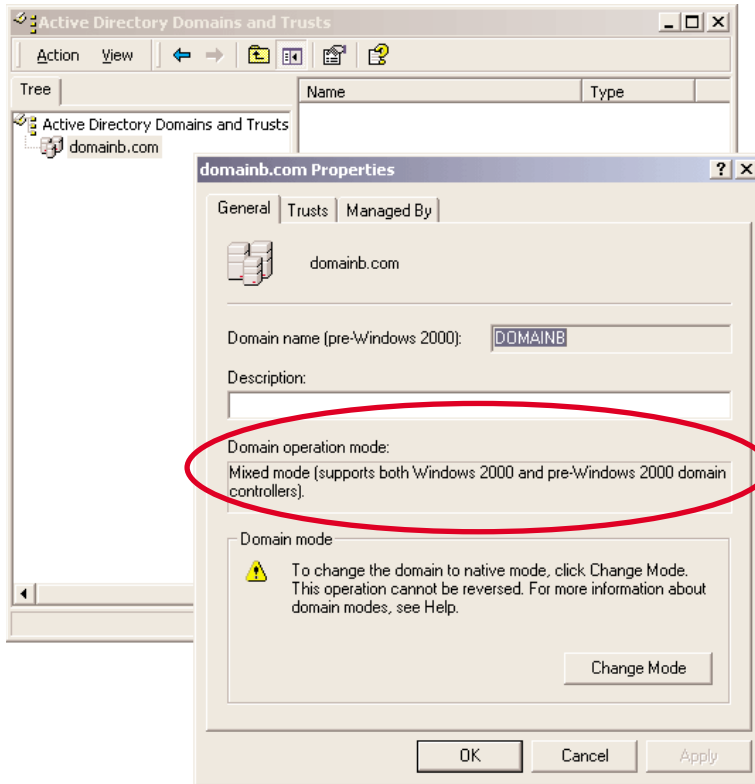
Now that I'm discussing how to analyze your particular scenario, let me remind you how to discover or verify your network's mode. To check your current configuration's mode, run Active Directory Domains and Trusts, which Figure 2.2 shows.

Figure 2.2
Active Directory Domains and Trusts



In the list of domains that appears, select the name of the domain whose mode you want to check and right-click Properties. The domain mode should appear. If you have any NT 4.0 BDCs, you're probably in Mixed Mode, as is the case with Domain B, which Figure 2.3 shows.

Figure 2.3
Ascertaining a domain's mode



Mixed Mode supports both Win2K and pre-Win2K DCs, which means that you can still add and remove NT 4.0 BDCs as needed. This capability is a good thing. You might have legacy applications that require you to keep NT 4.0 BDCs around until you find a Win2K or Windows 2003 solution.

Of course, much of the capability that you have with all Win2K DCs is missing in Win2K and NT Mixed Mode. (The next section details which capabilities you add if you make the switch to all Win2K DCs.) However, with the first Win2K DC, you get

- Group Policy support for Win2K and XP Professional clients
- IntelliMirror support for Win2K and XP Professional clients
- domain management capability through either Active Directory Users and Computers (Win2K) or User Manager for Domains (NT 4.0)

**Tip**

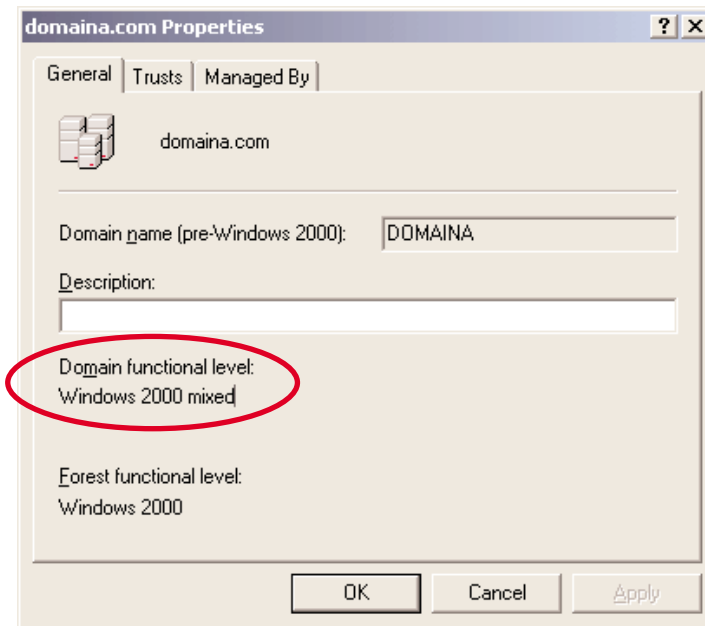
For an in-depth discussion of Group Policy and IntelliMirror, see my book *Windows 2000: Group Policy, Profiles, and IntelliMirror*. You can find information about the book at the URL below.

<http://www.sybex.com/sybexbooks.nsf/2604971535a28b098825693d0053081b/d15f21a26eaeed8588256bca0062a12f!OpenDocument&Highlight=0,moskowitz>

The promised land, as far as Win2K is concerned, is to get rid of all your NT 4.0 BDCs and have homogeneous Win2K DCs. Interestingly, new Windows 2003 domains are “born” into Win2K Mixed Mode. You can see Domain A’s initial mode – Win2K’s Mixed Mode – in the Windows 2003 domain’s Active Directory Domains and Trusts screen, which Figure 2.4 shows.

Figure 2.4

A new Windows 2003 domain’s initial mode



Therefore, if you build a new Windows 2003 domain from scratch, you could still, if you wanted to, introduce additional NT 4.0 BDCs. This capability might be helpful should you have legacy applications, such as a specialized account lookup program or a specialized piece of remote access equipment, that must reside on a BDC.

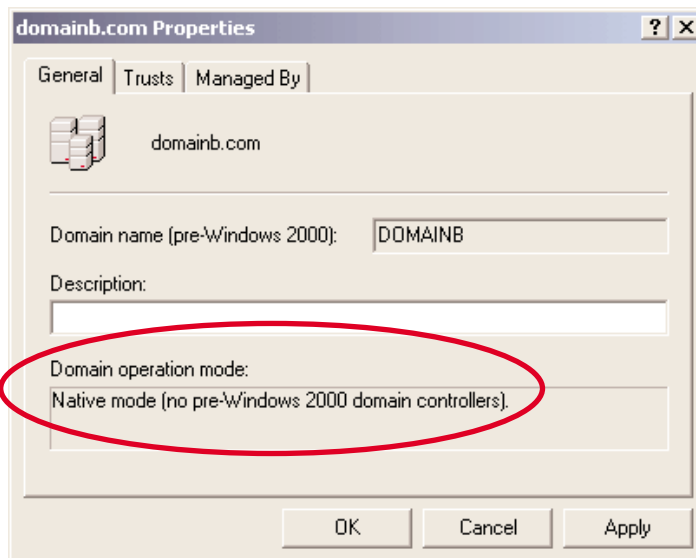
If You Have All Win2K DCs

After you leave the last NT 4.0 BDC in the dust, you can make the switch to Win2K's Native Mode, which introduces additional useful features.

- Universal Group support – This feature lets you assign groups from any domain to any other domain if the domains are in the same forest.
- Total Win2K-style replication – Without any NT LAN Manager (NTLM)-style replication to BDCs and with all your Win2K DCs using native AD replication, the replication process will now be more efficient.
- Additional capacity for security principals – Additional capacity lets you grow the database that holds users past the SAM's restriction of about 40MB. (You're still restricted even with one NT 4.0 BDC.) If you need this greater capacity, you know it!
- SidHistory – This feature lets a single account have multiple SIDs. (This capability is useful if you perform an NT 4.0-to-Win2K or an NT 4.0-to-Windows 2003 migration. Users might need to show alternate credentials to access data in their old domain.)
- Advanced Group nesting – You can now use multiple levels of nesting between different group types. Additionally, you can change the scope of domain local groups to domain global groups by clicking one button.

To make the switch to Native Mode on a Win2K domain, just click Change Mode, which Figure 2.3 shows. You'll be asked to confirm that you want to change the mode. If you answer Yes, the Domain operation mode changes with little fanfare, as Figure 2.5 shows.

Figure 2.5
Changing the domain's operation mode to Native Mode



Your Win2K domain is now in Win2K Native Mode, which lets you add Windows 2003 as well as Win2K DCs. Keep in mind, however, that Windows 2003 in Win2K Native Mode doesn't allow NT 4.0 BDCs.



Caution

When you make the switch to Win2K Native Mode, you effectively abandon any remaining NT 4.0 BDCs. They won't receive updates from your Win2K domain. If you don't disconnect the NT BDCs, they might introduce network errors (e.g., they might validate deleted users' access to your network).

If You Have All NT 4.0 Domain Controllers

Now we can discuss a unique case: You have *all* 4.0 NT DCs and you're considering switching directly to Windows 2003. You're not required to first upgrade your NT 4.0 domain (and therefore your NT 4.0 BDCs) to Win2K DCs before you move to Windows 2003. What do you need to know as you consider whether to skip the step of having Win2K DCs?

First, if you have all NT 4.0 DCs, you can still upgrade any NT 4.0 member server to either Win2K or Windows 2003. You might choose an upgrade for servers such as your SQL servers, Systems Management Server (SMS) servers, IIS servers, and Oracle servers. If you don't have any Win2K or Windows 2003 DCs, you'll encounter NT 4.0's inherent limitations, which include

- a SAM size restricted to about 40MB
- no Group Policy
- no IntelliMirror capability
- a single point of failure (If the PDC goes down, no users or administrators can update account information or change passwords.)
- the old replication model (BDCs pull from PDCs at scheduled intervals.)
- the need to reformat a BDC to remove its role as a DC



Note

A third-party tool, such as Algin Technology's U-Promote, can in most cases help you promote or remove an NT 4.0 BDC's DC status, leaving it a plain server. As with any tool, use U-Promote only if you have current backups on hand.



Tip

You can upgrade an NT 4.0 Server to either Windows 2003, Standard Edition or Windows 2003, Enterprise Edition. However, you can upgrade NT 4.0 Server, Enterprise Edition only to Windows 2003, Enterprise Edition.

Decision Point

At this point, if you're running all NT 4.0 DCs, you're ready to decide whether to bypass the Win2K DC step completely. You know that you can jump from NT 4.0 straight into Windows 2003 – but what else should you consider?

If you know that Win2K DCs won't ever – and I mean *ever* – be involved in your journey to Windows 2003 AD, you can take advantage of a special domain mode, Interim Mode. Interim Mode is useful in the unique scenario comprised of NT 4.0 BDCs and Windows 2003 DCs – no Win2K DCs allowed.



Caution

Interim Mode works only with NT 4.0 BDCs and Windows 2003 DCs.

Getting to Interim Mode

If you currently have 100 percent NT DCs and want to introduce your first Windows 2003 DC, how do you move into Interim Mode? You select it when you use the Active Directory Installation Wizard to upgrade an NT 4.0 domain's PDC. You choose the forest functional level for forests that won't contain Win2K DCs, as Figure 2.6 shows.

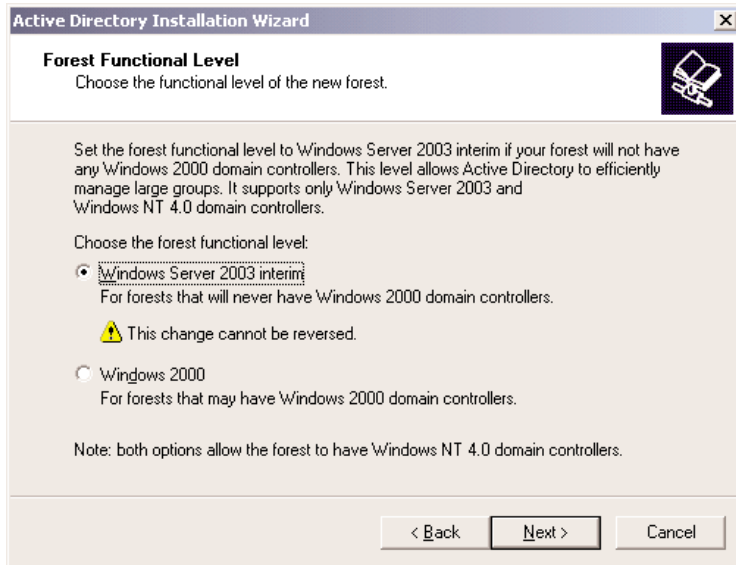
Why Does Interim Mode Exist?

Interim Mode compensates for a specific limitation of both Win2K Mixed Mode and Win2K Native Mode (one that doesn't occur with either NT domains or the Windows 2003 equivalent of Native Mode).

The problem lies in group account memberships. NT 4.0 domains let you maintain more than 5000 members in a security group – for example, in a Domain Global Group. However, after you've introduced Win2K DCs, the group account membership situation changes because Win2K DCs can't handle more than 5000 members in a group.

Windows 2003, on the other hand, can handle more than 5000 members in a group – just as NT can. Therefore, you can combine NT 4.0 BDCs and Windows 2003 DCs and use Interim Mode. Interim Mode also provides better replication – specifically between other Windows 2003 DCs.

Figure 2.6
Choosing Interim Mode



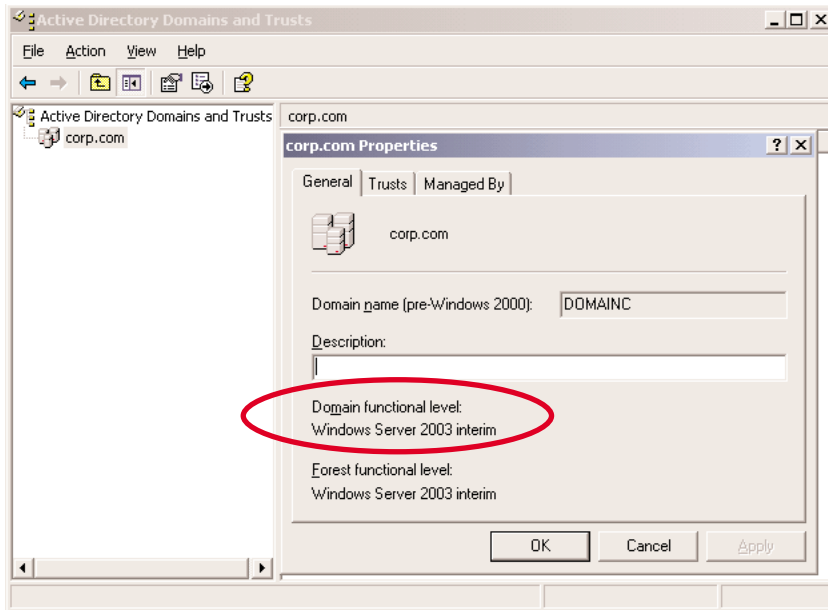
Note

The Active Directory Installation Wizard dialog box is titled **Forest Functional Level**. I discuss **Forest Functional Levels** later in this chapter. If you select **Windows Server 2003 interim** here, you're also changing the domain level to **Windows 2003 Interim** domain level.

When you upgrade an NT 4.0 PDC (to upgrade your NT 4.0 domain), Dcpromo will run automatically. As you can see above, the text lets you know that the setting is right for you *only* if you'll never have Win2K DCs. Also, notice the statement in the lower left-hand corner of the dialog box: *Note: both options allow the forest to have Windows NT 4.0 domain controllers*. In fact, you can include NT 4.0 BDCs until you make the switch to Win2K Native Mode or the Windows 2003 equivalent (described below).

After the upgrade is complete, you can see Interim Mode again, in Windows 2003's Active Directory Users and Trusts, which Figure 2.7 shows.

Figure 2.7
DOMAINC upgraded to Interim Mode

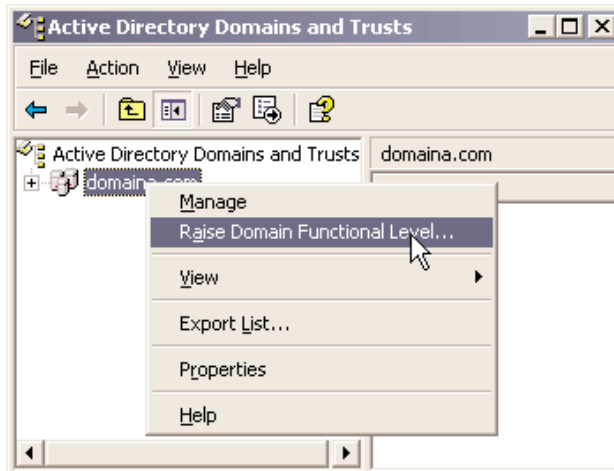


If You Have No Windows-based Domains

If you have no Windows-based domains whatsoever (i.e., in the case of a fresh Windows 2003 domain installation), you'll probably start with 100 percent Windows 2003 DCs. In that case, you would bring up your first Windows 2003 Server, run Dcpromo, and create your first domain.

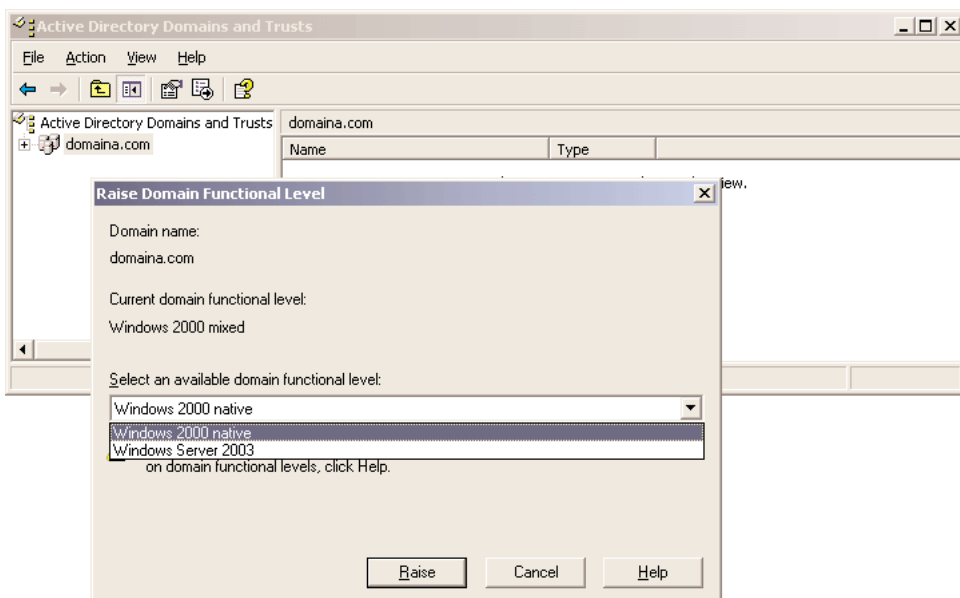
Assuming you won't need any NT 4.0 BDCs or Win2K DCs, you can get all the benefits of a homogeneous domain with Windows 2003 DCs at Windows 2003's domain functional level. First, however, because you create a Windows 2003 domain as a Win2K Mixed Mode domain, you'll need to "bump up" the domain's functional level. You raise the level through Active Directory Domains and Trusts by right-clicking the domain name and selecting *Raise Domain Functional Level*, which Figure 2.8 shows.

Figure 2.8
Raising a domain's functional level



Next, you can select the functional level you want to support, as Figure 2.9 shows. Your choices are to support a domain with Win2K DCs and Windows 2003 DCs or a domain with 100 percent Windows 2003 DCs.

Figure 2.9
Selecting an available domain functional level



Select the domain functional level you want, then click Raise. You can bump one level to *Windows 2000 native* or two levels to *Windows Server 2003*.



Caution

Raising the level is irreversible. That is, if you select *Windows 2000 native*, you can't go back to *Windows 2000 mixed*. If you select *Windows Server 2003*, you can't go back to either *Windows 2000 native* or *Windows 2000 mixed*.

After a domain is at Windows 2003's domain functional level, you get the following major additional features.

- InetOrgPerson becomes a user principal (I discuss this feature in Chapter 5: Windows Server 2003 Security Enhancements).
- Update logon timestamp: This feature lets administrators easily determine when a specific user logged on and to which DC. You'll find this information helpful for auditing purposes. I discuss this feature and a tool that helps you examine the attribute involved in Chapter 7: Command Line, Support Tools, and Resource Kit Tools.
- Domain rename feature (I discuss this feature in Chapter 8: Special Domain Operations).

Domain Level Review

You might find the different domain levels a little confusing. Table 2.1 offers a quick summary of Win2K and Windows 2003 domain levels.

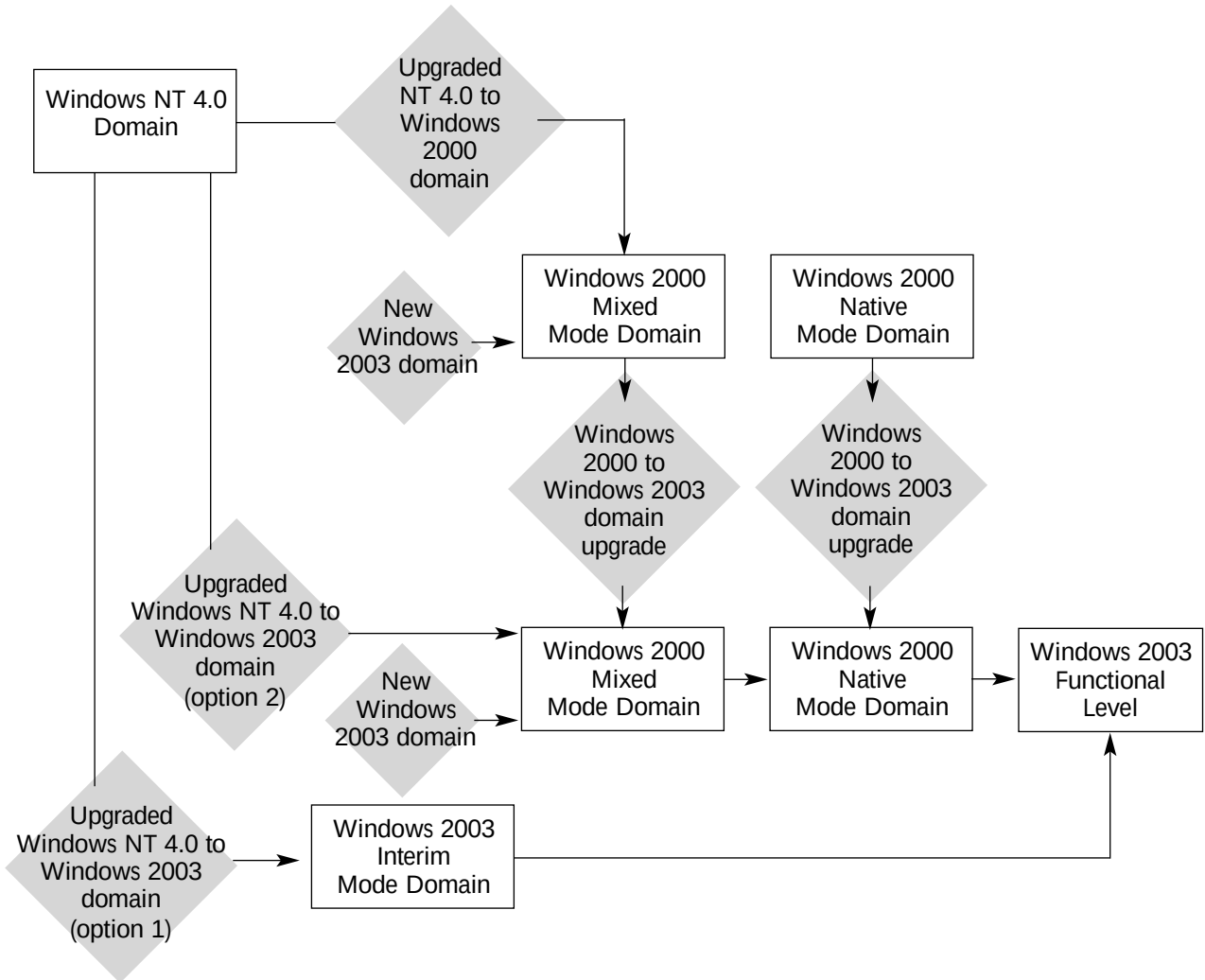
Table 2.1
Win2K and Windows 2003 domain levels

Mode or Functional Level	Machines Allowed	When useful	Features	Notes
Win2K Mixed Mode	Win2K DCs, Windows 2003 DCs, and NT 4.0 BDCs	When you have an application on an NT BDC on which your business depends	Group Policy and IntelliMirror for Win2K Professional and XP Professional clients	Both Win2K and Windows 2003 domains are created in Mixed Mode. NT 4.0 BDCs can participate in Win2K Mixed Mode.
Win2K Native Mode	Win2K DCs and Windows 2003 DCs	When you have a new Win2K domain, a new Windows 2003 domain, or a Win2K domain with new Windows 2003 DCs	Universal Group Support, SidHistory, SAM limit gone – replaced by 100 percent Win2K-style replication	NT 4.0 BDCs are excluded from this mode.
Windows 2003 Interim Level	Windows 2003 DCs and NT 4.0 BDCs	When you're upgrading an NT 4.0 domain and have NT 4.0 BDCs	Group size of 5000+ users, enhanced Windows 2003 replication to other Windows 2003 DCs	You can choose this mode only if you're upgrading an NT 4.0 PDC with a Windows 2003 CD-ROM. Win2K DCs are excluded from this mode.
Windows 2003 Functional Level	Windows 2003 DCs	When you're creating 100 percent new Windows 2003 domains without any older DC types	See the text below	Win2K DCs and NT 4.0 BDCs are excluded from this mode.

Domain Functional Level Diagram

Understanding precisely when you can progress to each domain level can be a bit daunting. The graphic in Figure 2.10 should help guide you – whether you have an NT 4.0 domain, a Win2K domain, or a Windows 2003 domain.

Figure 2.10
Upgrading from NT 4.0 or Win2K to Windows 2003



Caution

Let me remind you once more that domain upgrades aren't reversible. If you select Win2K's Native Mode, you can't go back to Win2K's Mixed Mode. If you select Windows 2003's Interim Level or Windows 2003's Functional Level, you can't go back to either Win2K's Native Mode or Win2K's Mixed Mode.

Working with Forest Levels

In the previous section, you saw that a Win2K domain and a Windows 2003 domain could each have its own domain-wide level. The same is true for a Windows 2003 *forest*. You create a new Windows 2003 forest at Win2K's forest functional level.



Tip

Interestingly, a Win2K forest just “is” – no distinction is made between particular modes. Only Windows 2003 forests make a distinction between Win2K's forest functional level and Windows 2003's forest functional level.

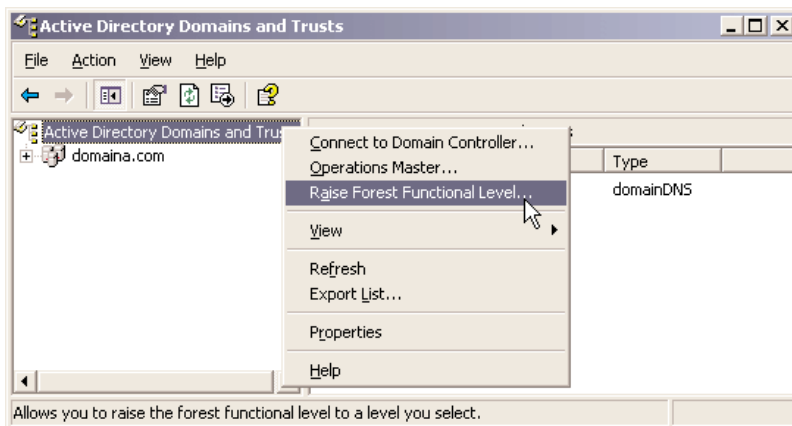
However, to get to the best features that Windows 2003 AD offers, you must first reach Windows 2003's forest functional level. To do so, you must ensure that

- all DCs are Windows 2003
- all domains are switched to Windows 2003's domain functional level

After you've completed that preparation, you can take it one step further. That is, you can throw the switch to bring the entire forest to Windows 2003's forest functional level – the Holy Grail of Windows 2003 AD.

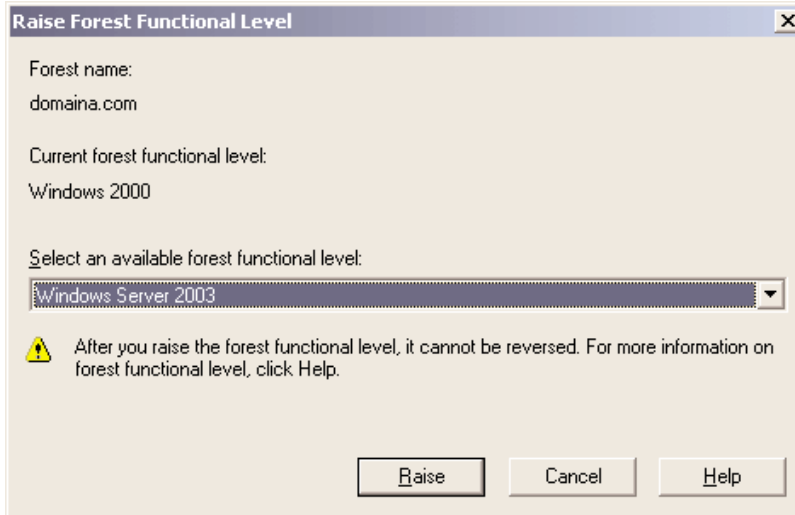
To raise the forest level, right-click the Active Directory Domains and Trusts root and select Raise Forest Functional Level, which Figure 2.11 shows.

Figure 2.11
Raising the forest functional level



After you've selected Raise Forest Functional Level, you'll see the current functional level of the forest, which Figure 2.12 shows. That level should be *Windows 2000*. If you run Win2K, *Windows Server 2003* will be the only functional level available.

Figure 2.12
Selecting Windows 2003's forest functional level



If you chose to perform an NT 4.0 upgrade into an Interim level domain and forest, you have two options: *Windows 2000 Server* and *Windows Server 2003*. Note, however, that you'll need to throw Windows 2003's domain functional level switch in each domain before Windows 2003's forest functional level is valid. Simply click Raise on the domain functional level you want, and you're done.



Caution

As is true in raising a domain's level, after you raise a forest's level, you can't reverse the move. That is, if you start with Win2K's forest functional level and you select Windows 2003's forest functional level, you can't go back to Win2K's forest functional level.

Windows 2003 Forest Functional Level Features

After you make the irreversible move to Windows 2003's forest functional level, you get a gaggle of new Windows 2003 AD features. Some features are "under-the-hood" enhancements, and others are features you can deploy to solve specific business problems.

Here are some enhancements you get "under the hood" with Windows 2003's forest functional level:

- **Linked Value Replication (LVR) improvements** – Under Win2K, you encountered a problem in replicating the membership of group accounts. If Stacey in the USA and Ralph in Great Britain modified the Nurses group membership at about the same time (a user initiated a second change before the replication function completed the first change), you could only guess which change would "win" in AD. Now those changes merge successfully.

- Global Catalog (GC) indexing improvements – Under Win2K, if you wanted to manually add a value to be contained inside the GC server (e.g., social security number), you could do so. , each GC would essentially dump its index and start re-indexing, which could cause massive network traffic among the DCs. Global Catalog servers now retain their indexes when a new attribute is added; the index adds only the change.
- Intersite Topology Generator (ISTG) improvements – Under Win2K, you faced a practical limit. At some point between 200 and 250 AD sites, you had to perform some special magic to add more sites. Oftentimes, adding more sites involved consultants and was expensive. Now, you can have literally thousands of AD sites without the system even breaking a sweat.

Here are some additional major features that Windows 2003's forest functional level offers:

- Domain rename feature – This feature sounds straightforward and self-explanatory; however, using the feature requires some background, as I explore in Chapter 8: Special Domain Operations.
- Cross-Forest Trust – If your forest is at Windows 2003's forest functional level and another company (or an unrelated organizational segment of your company) also has a Windows 2003's forest functional level forest, you can minimize the potential number of trusts by creating one cross-forest trust. I explore cross-forest trusts in Chapter 3: What's New in Windows Server 2003 Active Directory Management.
- Defunct Schema Object – In Win2K, if you had a schema addition and wanted to make a change, you had exactly zero options to fix the problem. Windows 2003's forest functional level changes the score a bit. I explore this feature in the next chapter as well.

Preparing for the Upgrade

If you currently have a Win2K forest with one or more Win2K domains, you'll probably want to upgrade them to Windows 2003 domains in a Windows 2003 forest. I've reviewed the domain and forest levels; now it's time to discuss preparing for the upgrade.

When you have Win2K domains, you use the Win2K schema. To use Windows 2003 domains, you must upgrade to the Windows 2003 schema. To upgrade your existing Win2K domains to Windows 2003 domains, you'll first need to have the right tool – which you'll then run several times. That tool is Active Directory Prep (Adprep). You'll find Adprep.exe on the \i386 directory of the Windows 2003 CD-ROM. You can choose to run Adprep directly from the CD-ROM or copy it to a network share or floppy.

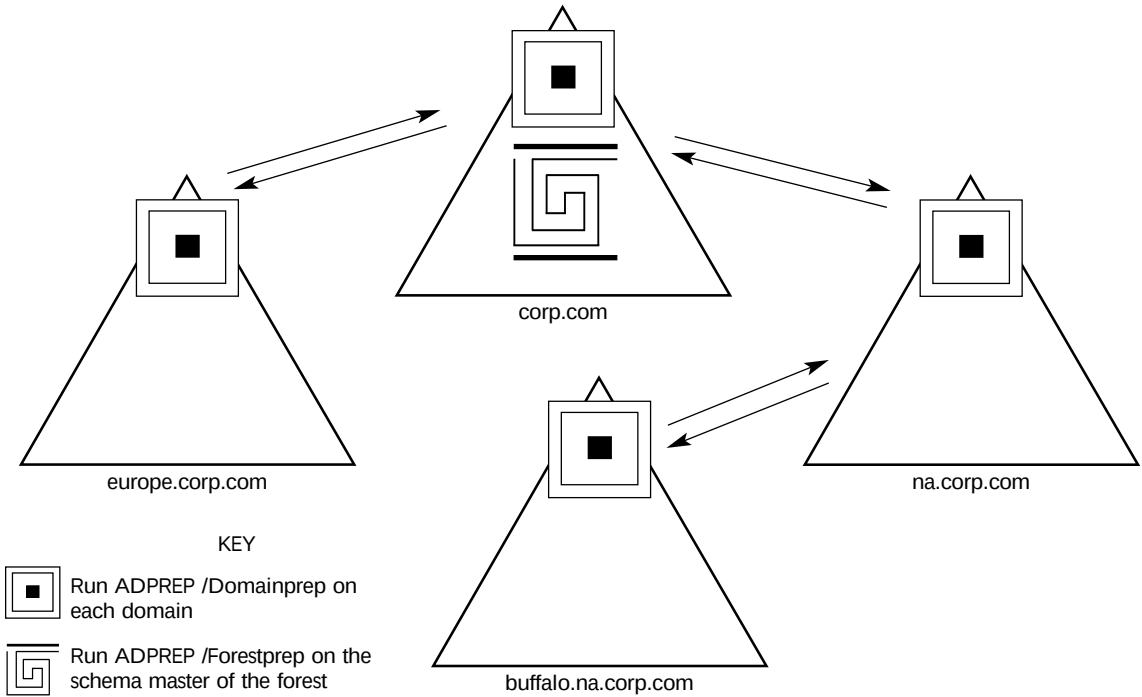
Using Adprep

Adprep's purpose is to upgrade the schema to Windows 2003 levels and give it a new revision number. You'll need to run Adprep multiple times:

- Run Adprep /forestprep – one time on the schema master of the root domain of the Win2K forest
- Run Adprep /domainprep – one time for each domain on the schema master of each domain

For example, if you have four domains, you'll run Adprep five times: once for the forest and once for each domain, as Figure 2.13 shows.

Figure 2.13
Running Adprep



Running Adprep /forestprep

To prepare the Win2K forest, you must run Adprep /forestprep on the schema master of the forest. Make sure that you have the proper service pack level loaded (see the Caution below).



Caution

You should have at least Win2K Service Pack 2 (SP2) loaded on all DCs before you continue. Win2K SP3 is preferred. You can proceed, however, with even SP1 (plus hotfixes).

Pop the Windows 2003 CD-ROM into the schema master, and run Adprep /forestprep. When you do, you'll see Adprep update the schema incrementally – from Version 13 of Win2K to Version 30 of Windows 2003, as the output in Listing 2.1 shows.



Tip

If your schema starts at a number greater than 14, someone might have already performed this step with a Windows 2003 beta or release candidate (RC).

Listing 2.1*Output from Adprep schema update*

```

X:\I386>adprep /forestprep
ADPREP WARNING:
Before running adprep, all Windows 2000 domain controllers in the forest
  should be upgraded to Windows 2000 Service Pack 1 (SP1) with QFE 265089,
  or to Windows 2000 SP2 (or later).

[User Action]
If ALL your existing Windows 2000 domain controllers meet this requirement,
  type C and then press ENTER to continue. Otherwise, type any other key
  and press ENTER to quit.

Opened Connection to SERVERB
SSPI Bind succeeded
Current Schema Version is 13
Upgrading schema to version 30
Connecting to "SERVERB"
Logging in as current user using SSPI
Importing directory from file "C:\WINNT\System32\sch14.ldf"
Loading entries.....
111 entries modified successfully.

[Some output removed for readability]

The command has completed successfully
Connecting to "SERVERB"
Logging in as current user using SSPI
Importing directory from file "C:\WINNT\System32\sch29.ldf"
Loading entries.....
6 entries modified successfully.

The command has completed successfully
Connecting to "SERVERB"
Logging in as current user using SSPI
Importing directory from file "C:\WINNT\System32\sch30.ldf"
Loading entries.....
15 entries modified successfully.

The command has completed successfully
.....
Adprep successfully updated the forest-wide information.

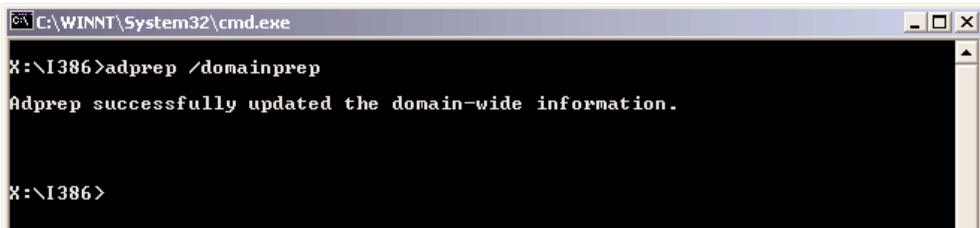
X:\I386>

```

Running Adprep /domainprep

You're now ready to run Adprep /domainprep. Microsoft recommends that you run the tool on each domain's infrastructure master. You should see the output that Figure 2.14 shows.

Figure 2.14
Adprep /domainprep output

A screenshot of a Windows command prompt window. The title bar reads 'C:\WINNT\System32\cmd.exe'. The command prompt shows the command 'X:\I386>adprep /domainprep' and the output 'Adprep successfully updated the domain-wide information.'. The prompt then returns to 'X:\I386>'.

```
C:\WINNT\System32\cmd.exe
X:\I386>adprep /domainprep
Adprep successfully updated the domain-wide information.
X:\I386>
```

You're now ready to upgrade your Win2K domain to Windows 2003. You can start with the recommended upgrade method: that is, begin with the PDC of the root domain, then upgrade each PDC in each domain. On the other hand, you could actually choose a Win2K DC and start your upgrade there.

Next: Window 2003 AD Management

In this chapter, I've reviewed the differences between NT, Win2K, and Windows 2003 – especially regarding AD domain and forest levels and the functions that each level provides. In Chapter 3: What's New in Windows Server 2003 Active Directory Management, you'll see what you can achieve after the upgrade. As I continue, I'll assume that you're working in Windows 2003's full forest functional mode. To prepare, take the steps that this chapter outlined in your test lab.

I'll introduce the new administration console and administration features, discuss cross-forest trusts, and begin to explore some of the management features that Windows 2003 AD offers. I hope you're riveted to your seat awaiting the next chapter!