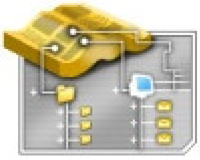
Windows Server 2003 Active Directory by Guy Thomas

Table of Contents

1) Logical Structure of Active Directory

Forest, Tree, Domain and Organizational Unit

Introduction



The purpose of this page is to introduce and define the terms used to design Active Directory. So put on your network architect hat and see how a Server 2003 forest is built.

Topics for the Logical Structure of Active Directory

Forest

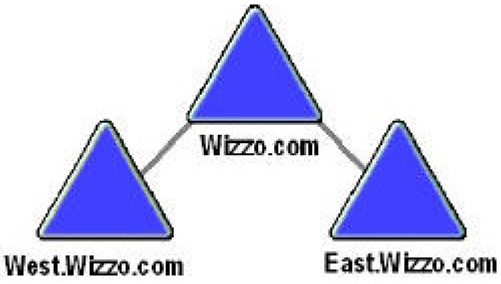
The Forest is the highest level in Active Directory.   Logically, a forest is a collection of domains all joined by parent child trusts. Another way is to think of a forest as a group of trees branching from a root domain. From a technical standpoint, all objects in the forest share the same schema definitions.

Recommendation

Take great care naming your first domain as this sets the name of the forest. Check the DNS settings in the System Icon, Computer Properties.

Trees

It is easy enough to define a tree: a group of domains that share a contiguous namespace. That means each domain in the tree has a common part of the domain name, and that they are joined by parent-child trusts. For Example East.Wizzo.com, West.Wizzo.com. In this case Wizzo.com is the tree.



Trees are difficult to pin down in the sense that there is no special Snap-In to configure them. The only way to get an idea of the tree structure is to look in the Active Directory Domains and Trusts, select the root domain, properties, then Trusts; now you should see all the trees.

Recommendation

As with most aspects of Active Directory, simple is best; so try and avoid deliberately creating trees. Multiple trees arise either through mergers or companies that have well know subsidiaries. Chocolate.com and Buscuit.com would be two different trees because they have no common namespace.

Domains

The domain remains the basic unit of Active Directory. From a technical point of view, domains are the security boundary of Active Directory. From a practical point of view this means that security policies set in at the domain cannot be changed at the OU level.

Users do not need to know which tree, forest or even OU that they belong to, but they should know which domain to select at logon. The modern way for the user to logon is to enter their User Principle Name (UPN) in the domain logon box. The UPN name looks like an email address; for example guyt@Wizzo.com.

Domain controllers need to replicate directory information with all other domain controllers in their own domain. If this replication is sluggish or chokes a slow link, then first try separate sites, if that solution does not work then consider separate domains in each geographic location.

Recommendations

Make it your reflex to have one domain. As you can now have at least 10 million objects in a domain, only allow a second domain if there is a very good business case, such as a multinational company with different security requirements.

Create and use UPNs so that users can logon anywhere in the forest.

Organizational Units

In the early days, Active Directory Organizational units were under used; NT 4.0 Administrators were happy to create lots of domains and continued this questionable practice in Window 2000. By 2003, enlightened administrators see the advantage of arranging users in OUs. Two other benefits are, firstly, you can apply different Group Policies for different OUs, secondly you can delegate routine tasks to local administrators in each OU.

Recommendations

Take care when you design your top level of OUs. Segregate users by geographic location or department. Make it your reflex to create a new OU rather than a new domain.

What's new in Server 2003

Forest Trusts. You can create trusts between forests

Once you Raise the Forest Level to Server 2003, then you can rename domain controllers or even the domains themselves.

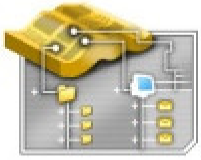
Use the control or shift key to select and change one attribute in many users. (You could do this in NT, but not Windows 2000)

Summary and Recommendations

1. Take great care naming your root domain. Plan how to link domain names with DNS zone names.
2. As with so much in Active Directory, simple is best; therefore, try and avoid deliberately creating trees.
3. Make it your reflex to deploy only one domain where ever possible.
4. Create and use UPNs so that users can logon anywhere in the forest.
5. Plan your top level of OUs. Segregate users by geographic location or department. Make it your reflex to create a new OU rather than a new domain. See also Organization Units and Delegation.

2) OUs and Delegation

Divide and rule. Plan your Organization Units.



Introduction to Delegation and OUs (Organization Units)

Active Directory has created a new role called Network Architect. One task for the Network Architect is to design OUs and delegate permissions. Delegation is versatile; for instance, at the DOMAIN level you could assign the HelpDesk Global group the permission to reset any password in the entire domain. Whilst at the OU level, you could delegate local administrators complete control of users in their own department. With this arrangement local administrators can create new users, groups and computer objects, but only in their own OU.

Topics for Delegation and OUs

1. **Three aspects to planning your OUs**
2. **What's New**
3. **Getting Started**
4. **Summary and Recommendations**

One problem with NT 4.0 domains was that often there were too many of them. This came about partly because of the SAM limit of 40 MB, but more likely because each manager wanted total control of their own department. You can solve this problem in Windows Server 2003 by creating OUs and then allowing department control over their own users and OUs. Only create more domain if there is a good business case, for example: multinational company with different languages or vastly different security settings.

Three aspects to planning your OUs

1. Organize users by arranging them into OUs
2. Delegate mundane tasks like resetting passwords
3. Plan desktops through group policies

1. Organize users by arranging people by OUs

By default all users are created in the Users folder. Much better to 'file' users into OUs so that you can manage them more easily. Once you have organized the user accounts you can apply the same techniques to computers and groups.

2. Delegate mundane tasks like resetting passwords

Since resetting passwords because of account lockout is not difficult, you can delegate to some who is in authority but not necessarily a server specialist. Once you establish OU's and delegation then a local administrator or power user can reset the password and thus leave you to get on with more interesting work. With delegation, the domain Admins decide which local administrators have control over which tasks. For the more experienced administrators, you could allow them to create user accounts for new joiners, and disable accounts for those who have left.

Delegation Tactics

Firstly create groups with delegation in mind.
Example: Global Group = HelpDesk to allow password changes.
Global Group = HR Deputy to add more users.

Secondly consider the tactical question: "Do you delegate at the Domain level or at the OU level?"
Example: At the **Domain** level, delegate HelpDesk, to Reset Passwords for everyone in the domain.
Example: At the **OU** HeadQuarters, delegate HR Deputy to create accounts for new staff.

Active Directory is flexible so you can do both, or even change your mind if the strategy needs adjusting.

3. Plan desktops through group policies

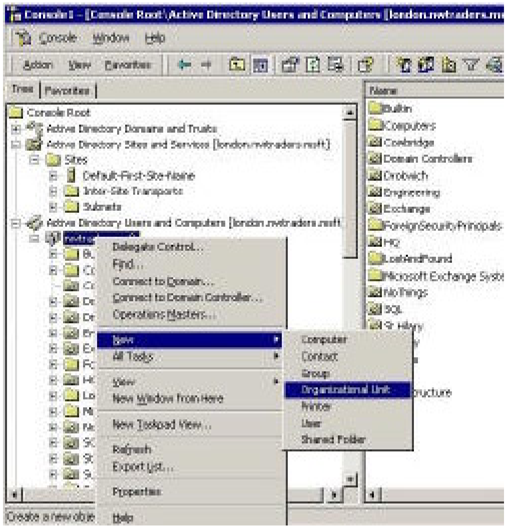
Incidentally the default Users container is not an OU and so you cannot set group policies on that container object. Group policies are the key to controlling the user's desktop and assigning the software they need. Organizational units are the best place to apply most of the policy settings. The exceptions are security policies which must be set at the domain level. By creating OU's you can fine tune which software is assigned to which users. For instance, customer facing users will need stricter controls over their wallpaper and desktop icons than the back-room team in tech support.

What's New

OU's and delegation are virtually identical in Windows Server 2003 and Windows 2000. The only relevant new features are improvements to group policies, and they are covered on a separate page.

Creating OUs - Getting Started

Go to the Active Directory Users and Computers, select 'Domain', Right Click, New OU. Then to delegate Right Click the OU and Delegate is the first item on the shortcut menu.


Console1 - [Console Root\Active Directory Users and Computers [london.nwtraders.ms

Firstly, make sure that the Security Tab is available on the OU Properties. On the above diagram you would go to the View (menu) and select Advanced Features. Now go back and check the OU, Properties, Security (tab), Advanced should now be there.

When you create OUs balance geographic sites with departmental structure.
Example: Create a top level of OUs reflecting the branch offices, then nest departments inside each branch OU.

Delegation - Getting Started

When you right click on an OU or the Domain, you see 'Delegate Control' is the first item on the menu. Once activated, the wizard will lead you through the steps to select the group, then choose the tasks to delegate. It pays to run the wizard a number of times, just to see all the options available.

Summary and Recommendations

1. When you create your top level OU's, consider whether they will contain skilled staff to whom you can delegate routine tasks such as resetting passwords.
2. The two main choices at the top level are by geographic location or by department.
3. Do not use more than one level of OU nesting.
4. Remember to design your OU structure with Group Policies in mind.
5. Decide in which OU's will you place the computers and groups.
6. Delegate by group rather than individual user.

3) Group Policy

Desktop configuration explained through the eyes Mr Men!

Introduction to Group Policy.

I am not a great committee man, but if there is one committee that I would volunteer for it would be the policy committee. This is because Group Policies give you complete control of the users' security and desktop settings.

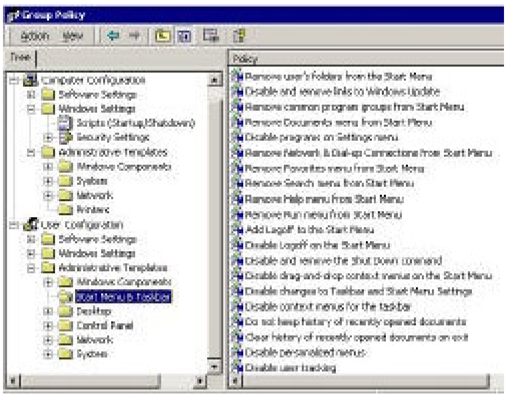
When you set policies in Active Directory, you take on a number of roles or wear many 'hats'. To digress for a moment, in England there was (is) a series of books for young children called 'Mr Men' books, I remember reading about Mr Angry, Mr Sensible and whole series of others. Well, I have adapted this idea, and I challenge you to wear different 'hats' you need to configure policies.

Topics for Group Policy

1. **Mr Nasty - Classic desktop lock down**
2. **Mr Nice - Assign Software**
3. **Mr Packer - Create .msi packages**
4. **Mr Clever - Redirect Folders**
5. **Mr Smart - Use Policies to apply Logon Scripts**
6. **Mr Tester- Create a Special OU for practice**
7. **Mr GPMC - What's new in Server 2003**
8. **Mr Summary - Review and Recommendations**

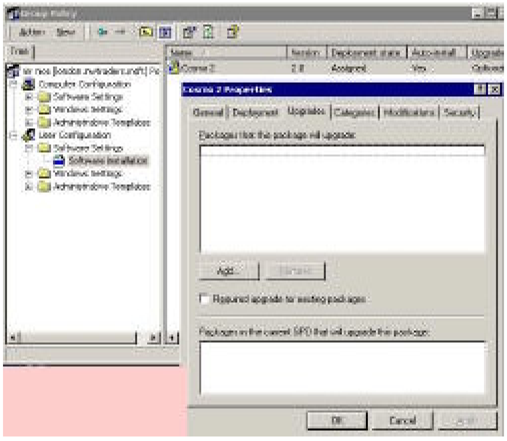
Mr Nasty

The role of Mr Nasty is to screw down the desktop as much as possible. Mr Nasty configures settings like 'Remove the Run Command', or 'Disable Display in Control Panel'. You should use Mr Sensible to moderate Mr Nasty and leave the users settings that are harmless.   When you are wearing the 'Mr Nasty' hat, check out these areas: Windows Components, System, Network, Printers, Start Menu & Task bar.



Remove user's Folders from the Start Menu
Disable and remove links to Windows Update
Remove common program groups from Start Menu
Remove Documents menu from Start Menu
Disable programs on Settings menu
Remove Network & Dial-up Connections from Start Menu
Remove Favorites menu from Start Menu
Remove Search menu from Start Menu
Remove Help menu from Start Menu
Remove Run menu from Start Menu
Add Logoff to the Start Menu
Disable Logoff on the Start Menu
Disable and remove the Shut Down command
Disable drag-and-drop context menus on the Start Menu
Disable changes to Taskbar and Start Menu Settings
Disable context menus for the taskbar
Do not keep history of recently opened documents
Clear history of recently opened documents on exit
Disable personalized menus
Disable user tracking

Another traditional role for Mr Nasty is to configure the Security Settings. Here is where you decide the Password length, duration, and lockout settings. You may be familiar with these security settings from your NT 4.0. Be aware that security must be set at the domain level. I know the same settings appear in the OU's but do not be deceived, if the users logon to the domain, the only security settings that apply are those in the Domain Group Policy container.



Mr Nice

Cultivate Mr Nice, because he will Assign all the programs a user needs for work. If there is a business case for an application then ask Mr Nice to create a Policy and deliver the package to the Start Menu. Mr Techie likes this approach because he can then apply service packs and upgrades from one central place. Mr Nice operates from the Software Settings folder. If you want everyone who logs on to use an application, then Assign it to a computer; however if the user needs special software wherever they logon, Assign it at the User Configuration folder (see diagram).

Trap!

If you choose the Computer Configuration, make sure that computers you think you are configuring, are in the same OU as the policy you have in front of you.

Mr Packer - Packaging the Software

Most modern software comes as .msi (Microsoft Installer) format. These new (ish) .msi packages need no alteration - just assign them.

The real benefit of assigning software comes when you have to apply an upgrade or a service pack. Mr Packer simply creates another package and re-configures the Group Policy settings.

However, if you have older software, use WinINSTALL LE to create .msi packages for your policy. You will find the packaging programme on the Windows **2000** Server CD \VALUEADD\MGMT\WINSTLE. However WinINSTALL does not appear to be on the Server 2003 CD so check the website if you need a lite version.

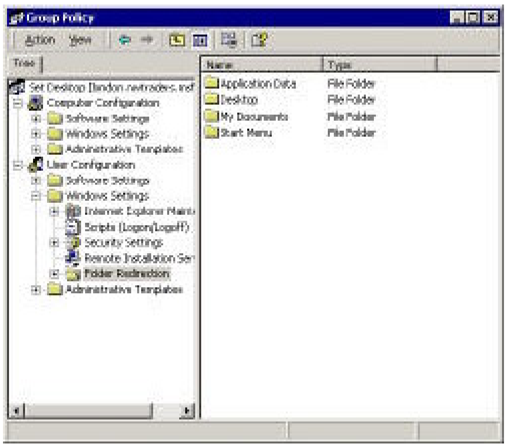
Guy's advice

I believe that you should remove settings that the users have no business to fiddle with, whilst leaving them settings that are innocuous. For instance why not allow them the Screen Save, and Change Wallpaper tabs?

Mr Clever - Folder Redirection

With all new software, be prepared for a change in mind-set. In the case of user's home drives, switch from using mapped network drives and try redirecting the 'My Documents' to a file server.

With Folder Redirection there are many options and several tactics. You need to decide whether to redirect just the 'My Documents' or include the 'My Pictures'. I like the tactic of giving each user their own 'My Documents' using the %username% variable. e.g. \\server\share\%username%.



Name	Type
Application Data	File Folder
Desktop	File Folder
My Documents	File Folder
Start Menu	File Folder

Mr Smart - Uses Policies for Logon Scripts

Mr Smart applies Logon Scripts via Policies. Whilst you can still apply Logon Scripts through the individual User, Properties, Profile tab, use group Policies instead.

Indeed, you may find less need for the old fashioned logon scripts which map drives and printers, instead you can achieve the same results by using group policies.

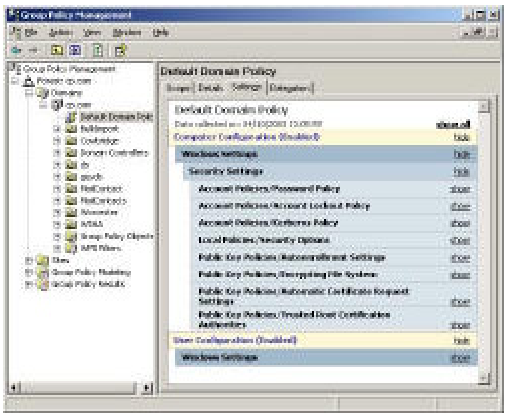
Mr Tester - Create a special Test OU

To test Group Policy create a special OU, then go to Properties, Group Policy (Tab), New (Policy), Properties. It will take about 10 days of practice to become an expert; in fact part of the 'rites of passage' is locking yourself out! That is why I suggest you start with a practice OU and leave the Default Domain Policy alone until you are experienced.

Mr GPMC

This Group Policy Management Consol is one of the best new features in the whole of Window Server 2003, it gives you complete control over all policy settings. The GPMC transforms management of policies. The only surprise is that you have to get a copy from Microsoft's Site, and that it's not available on the Server CD.

As well as the new interface there are 150 new Group Policies in Server 2000; these are in addition to the 250 new policies for XP compared with Windows 2000 professional.



Default Domain Policy

Default Domain Policy

Data collected on: 14/10/2003 13:05:59 show all

Computer Configuration (Enabled) hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy show

Account Policies/Account Lockout Policy show

Account Policies/Kerberos Policy show

Local Policies/Security Options show

Public Key Policies/Autoenrollment Settings show

Public Key Policies/Encrypting File System show

Public Key Policies/Automatic Certificate Request Settings show

Public Key Policies/Trusted Root Certification Authorities show

User Configuration (Enabled) hide

Windows Settings show

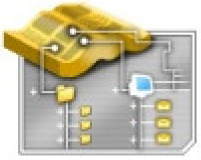
A trivial change is 'No Override' becomes 'Enforced' in Server 2003.

Mr Summary - Review and Recommendations

1. Get a test network to practice with Group Policy. It's a 'right of passage' that you will do something silly like lock out the administrator, learn all your mistakes on a test network.
2. Create a purpose built OU and special user to test group policies.
3. Take time to develop a vision. Ideally, you need a techie to check the settings and manager to concentrate on what the desktop should look like.
4. Remember Mr Nice and make it your reflex to roll out software through group policies.

4) DNS

"Those who do not learn from the mistakes of history are doomed to repeat them."
George Santayana



Introduction to DNS in Windows Server 2003

This page concentrates on configuring DNS for Active Directory. DNS plays a vital part of planning Active Directory names, and once Server 2003 is up and running. When ever you get name resolution problems, check DNS settings first.

DNS Topics

The Primary Purpose of DNS

Sometimes, particularly in troubleshooting, you have to go back to basics. Keep in mind that the primary point of DNS is to map a server's IP address to a friendly name. E.g. 195.209.12.50 Wizzo.com

Users need resources such as Kerberos authentication for logon and a global catalog to find computers. These resources are on servers with IP addresses. The extra dimension of DNS with Active Directory is the _SRV records. These service records tell you not only the server's IP address but also the services that it offers.

User's perspective - "I want to logon"

DNS with Active Directory - "I will look in the _SRV records for a server which offers Kerberos authentication"

DNS host record - "Here is the IP address of that server you need"

Importance of Naming and DNS

Naming your Active Directory Forest

It is crucial to understand all the implications of your naming conventions, especially the relationship between your domain name and DNS name. Learn from the mistakes of others. One urban myth has it that all the first 10 companies who installed Windows 2000 Active Directory, all had to go back to the drawing board and start again. What was their problem? In each case, they got their naming strategy wrong. (Or they did not have a strategy?)

The first question is, will you use an existing DNS name? And the second question is, if you are using and existing domain name will you use the same name for your first domain. A supplementary question, will the Root domain, be blank or will it be your HQ domain? There are no right or wrong answers to these questions, what I am saying is that once you make your decisions you have detailed plans to ensure it works and that you do not have to rip it all up and start again.

How many domains do you need, I do have a view here - as few as possible. Good reasons for having more than one domain, multi national company, incompatible security needs, different language versions of Windows 2003. Bad reasons for having a new domain, there is a new manager in division, a region wants complete control of its IT.

If you do find this planning too much, then either make a single domain work for you, or else employ a network architect who is used to resolving these naming dilemmas.

DNS names and Active Directory names.

The confusion arises because both DNS and Microsoft's Active Directory use the domain word. For clear thinking, it may be better refer to DNS as having zones and Active Directory having domains. That said, it is often a very good idea to have the DNS zone and the Active Directory domain share the same name. For example, DNS **zone** Wizzo.com, Active Directory root **domain** Wizzo.com. However, this arrangement can add to confusion unless you are clear about the distinction between DNS **zones** and Active Directory **domains**.

Here are some suggestions for naming objects. However, a better idea is for you to create your own naming checklist.

1. DNS Zone name - Wizzo.com
2. Active Directory - Root Domain Wizzo.com
3. Tree - Wizzo and TopBanana
4. Child domain Son.Wizzo.com
5. Sites - Midlands, North
6. Domain Controllers - DC_Red
7. Organizational Units - Top Level, Second Level
8. Users naming convention - LastNameFirstName
9. Group naming convention - Global Managers

Configuring DNS

DNS Registration and Query.

The whole purpose of DNS is to respond to queries. Remember the request for a Kerberos logon server? The XP machine contacts its DNS server and wants the IP address of a Kerberos server. Either the DNS server has the _SRV and host record itself, or it forwards the query to another DNS server. You must decide what records each DNS server holds and how much forwarding to allow to which other DNS servers.

Registration, on the other hand, is the automatic addition of host records in DNS. Configure your clients to register automatically with at least one DNS server. For the average client these DNS settings are best configured using DHCP.

In practical terms, both Registration and Query are configured through the TCP/IP property sheet.

Practical configuration of DNS and DCPROMO

Here is the scenario, you are about to install your first Active Directory domain controller. Remember that whenever you install Windows Server 2003, it begins life as a member server. To install Active Directory go to the Start Menu, then Run, DCPROMO and so create a domain controller. However, before you do that, check out DNS.

Begin in the System Icon, Computer Name (Tab), Change, More... Primary DNS Suffix of this Computer. Make sure the settings are as per plan.

Double check the Network Connections, Local Area Network, TCP/IP properties, Use the following DNS server address, does this point to itself, or to the correct DNS server? I would fill in both DNS server boxes if you have two DNS servers.

Install DNS through the Add or Remove Programs, Windows Components, Networking Components, Details - DNS. If this were your first server, I would run DCPROMO without any more configuration at this stage. My tactic is to let the Wizard add and populate the Forward Lookup Zone.

Once DCPROMO installs Active Directory, I would check that at least four _mcsdcs records are created; if not I would stop, then start the Netlogon service check again. Check the Event Log; examine the System and DNS logs for error messages. If still no _mcsdcs records appear, then I would reboot the server, take a 10-minute break and look again in DNS.

Experience tells me that either DCPROMO works fine, in which case there is no problem, or else installation is very stubborn. If still no sign of Active Directory records in DNS, I would run DCPROMO, demote and start again at the beginning. In the case of a test installation, I would change the Computer name and the domain suffix before trying again.

Post installation DNS checks

1. Once Active Directory records arrive in DNS, I would create the reverse lookup zone and test it with NSLOOKUP.
2. Select DNS in your MMC, or via the Administrative tools if you prefer, check the Event Viewer, which is now just under the DNS server object. Look up any suspicious error messages in TechNet.
3. Right click the DNS server, select Properties, Monitor (Tab), now press Test Now. Should the Recursive query fail, and then investigate the Root Hints. (I have never seen the Simple Query fail.)
4. If you are not connected to the internet. You may wish to create a '.' (dot, period, full stop) root domain and point it to your domain.
5. Many of us believe that you have not proved Active Directory is working properly until you have installed a second domain controller and seen replication of user accounts between the two domain controllers.
6. Finally set a date to switch to 'Raise Domain Functional Level'. In Windows 2000, this was called switching to Native Mode, but now in Server 2000, there are more options and the name has changed to Raise Level. When you have no more NT 4.0 BDC, raising the domain level turns on features like universal groups, group nesting, RAS Policies as well as more efficient directory replication.

What's new in Server 2003

All the major changes like Dynamic DNS and Active Directory integration happened between NT 4.0 and Windows 2000. In Server 2003, the changes amount to tidying the menus and interfaces in the DNS Server object. For example, the Event Viewer is now under the server to remind you to check for DNS errors; Cached Lookups are visible without having to select advanced objects.

Summary and Recommendations

1. Appreciate the difference between a DNS zone and Windows Server 2003 domain
2. Understand what happens during DNS querying and registration
3. Allow DCPROMO to configure the _SRV records
4. Manually create a reverse lookup zone
5. Check the properties of the DNS Server object
6. Master NSLookup for testing and troubleshooting

5) Installing Server 2003

Build your Active Directory Servers with care

Introduction to Installing Active Directory

The strategy with deploying Active Directory is to build a member server first, then run DCPROMO and install Active Directory itself. I do recommend you read the Logical Structure and DNS section and produce a plan before you actually install Active directory.

Installation Topics

Which 'flavour' of Server 2003 do you need?

Here is the range of Windows 2003 products that are available:

1. Standard Server - Classic file and print server could be your Domain Controller
2. Enterprise Server - Application server support for clustering
3. Datacenter Server - More of everything! Processors, memory and clustering
4. Web Server - For ISP's only available through specialist retailers
5. 64 Bit version - one day we will all be choosing this instead of the 32 Bit version
6. (XP Professional - Desktop replacement for Window 2000, Window 98, NT 4.0 Workstation)

Notes on choosing your version.

The key feature of the Enterprise Server is clustering. Beware that you cannot (and would not want to) install Active Directory on the Web Server. Datacenter can only be purchased as part of a hardware / software package, and is not sold on CD.

When you upgrade, you must upgrade like for like; Enterprise W2K to Enterprise W2K3 works. You cannot mix and match, unfortunately this is not a chance to upgrade Standard to Enterprise server.

Note: The Datacenter version is only available from selected manufacturers; it comes as a total package; multi-processors RAM and Windows Server 2003 Datacenter Server pre-installed. You cannot buy Datacenter on CD. Rumour has it that less than 100 Datacenters have been sold worldwide.

Installing Windows Server 2003 - Member

Quick, slow, quick quick slow, that is how the install seemed. The menus were very like XP with excellent PnP and comprehensive driver support.

All the questions that the wizard asked were straightforward and easy to answer.

I particularly liked the timer screen telling me how long to go. My criticism is, there could be a second clock to tell me how long until the next user intervention. What happened to me was I left with 34 minutes remaining, only to return half an hour later with a screen asking me to choose a time zone, and still 29 minutes to go.

As I am nearly always online, the product activation was easy, slick and asked for no personal information.

Installing Microsoft software
Guy's degree of difficulty

Hardest Install= 10
9 Exchange 2000
7 SQL 2000
6 NT 4.0
4 Windows 2000
3 Windows 2003 Server
2 XP
Easiest Install = 0

TIP For many years my cry has been: 'You never have a big enough C:\ drive', this time I went for 10GB. (After 3 days I had used 6.5GB)

Post installation considerations

Check the system logs in the event viewer. Then plan the role for your member server.

A long time ago I started with Windows v 2.0 and each Microsoft product since has its own personality, what struck me first with Windows Server 2003 was that it wanted me to tune it for a particular role: File and Print, Application or Domain Controller. This was the first time that I have seen this up front tuning and I liked it.

Once you have built your member server, you are ready for the main event: Active Directory.

Installing Active Directory

With installations, 7 minutes of planning will save an hour for rework. The secret of troubleshooting Active Directory installs is mastering DNS. I find NSLookup invaluable, also Ipconfig's new switches /registerdns and /flushdns are handy.

Procedure for creating a Domain Controller

The key to success is preparation. Decide your DNS and enter the name in the Computer Name Tab in the System Icon (Windows Key ⊞+ Pause). Whilst this section deals with the nuts and bolts of an installation, take care to design your Active Directory forest, for example, account naming strategy, top level OUs, group policies.

Now you are ready to run DCPROMO.

DCPROMO decisions

To call for the Active Directory Installation Wizard, Start, Run DCPROMO and answer these questions:

1. New Domain - or Replica? (This means another DC in the same domain)
2. Domain Tree in existing forest - or New Domain Tree?
3. Domain in New Forest?

Best practice

Remember that the Active Directory can grow so make sure the partition has at least 300 MB of free space for NTDS.dit itself, and 100 MB for the log files. Talking of the logs, install the edbxxx.log files on a separate disk.

Post installation considerations

To verify that installation has run smoothly check the following:

1. DNS _SRV record: _msdcs, _sites, _tcp, _udp. Also the GC, DC records are essential for users to find the global catalog and domain controller in order to logon. If these records do not appear, try stopping and starting the Netlogon service.
2. Run %systemroot%\sysvol and look for domain folders.
3. Check the System and Directory Service Event logs for error messages.

Demotion back to member server

If the worst comes to the worst, run DCPROMO to demote, then try again making different decisions.

What is new in Windows Server 2003?

ADPREP

ADPREP is a built-in command line tool that will prepare the schema ready for the main installation. It does not actually install the NTDS.dit files but it does prepare the forest or the individual domain for Active Directory.

ADPREP /forestprep

ADPREP /domainprep

DCPROMO /adv

If you already have a working domain controller, backup the system state, go to a member server, run DCPROMO /adv then point the wizard to the backup files

Summary and Recommendations

1. Plan the names for your domains and servers

2. Master DNS
3. Make sure you have plenty of disk space on the C:\ system partition
4. Consider creating replica domain controllers from a backup of the first server.

6) Raise Domain Level

Set a date to raise your domain from mixed mode.

Introduction to Raise Domain Level

Why is understanding raise domain level important? Because if you don't master it you will be missing out on Server 2003's new features. Once you discover how raise domain level works, then you can move on to raise forest level and unleash even more capabilities.

Topics for Raise domain level

Raise Function Levels in Windows Server 2003

The purpose of this page is to explain how the terms 'Mixed and Native mode' apply in Windows Server 2003. Actually, the terms mixed and native have been superseded by 'Raise Function Level'. I will also point out some of the benefits to switching the higher levels.

There are two separate aspects of Raise Function Level to be aware of. One aspect is the domain and the other is the forest. The key to understanding the concepts is to pay careful attention to these four words, **domain, forest, 2000** and **2003.**

Firstly, a Windows Server **2003 domain** can have a mixture of domain controllers: NT 4.0 BDCs, Windows **2000** DCs and naturally, Window Server **2003** DCs. (DC = Domain Controller)

Secondly, the **forest** may have all **domains** at the pure Window Server **2003** level. Alternatively, a **forest** can have **domains** running Window **2000** mixed or **2000** native **domains**.

Domain Function Levels - (Mixed and Native)

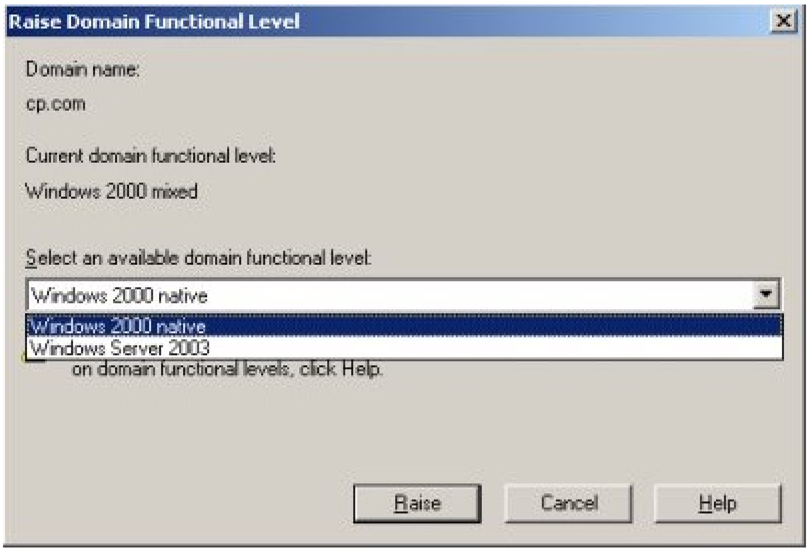
There are now four domain 'Levels' that a Windows Server 2003 can operate in. Whilst it is easy to understand what each level means, it takes time to learn Microsoft's terminology.

1. **Windows Server 2003.** All Server 2003, no other domain controllers. However, even in this level, the whole range of clients and member servers can still join the domain.
2. **Windows Server 2003 Interim.** NT4.0 servers and Window Server 2003 (no Windows 2000). This level arises when you upgrade an
3. NT 4.0 PDC to Server 2003. Interim mode is important where you have NT 4.0 groups with more than 5000 members. Windows 2000 does no allow you to create groups with more than 5000 users.
4. **Windows 2000 Native.** (Yes Windows **2000** native) allows Windows 2000 and 2003 servers (no NT 4.0).

5. **Windows 2000 Mixed.** (Yes Windows **2000** mixed) allows NT 4.0 BDCs and Window 2000. Naturally, Windows 2000 mixed is the default function level because it supports all types of domain controllers.

Key term - Raise Domain Functional Level

Windows 2000 mixed mode means that there is at least one NT 4.0 BDC somewhere in the Forest. To make raise the level, click the Domain object in Active Directory Users and Computers and select: Raise Domain Functional Level. Here is the menu you see:



Raise Domain Functional Level

Domain name:
cp.com

Current domain functional level:
Windows 2000 mixed

Select an available domain functional level:
Windows 2000 native

on domain functional levels, click Help.

5 Features Available in Windows 2000 Mixed Level

While Windows Server 2003 mode is the ultimate goal, there are new benefits of deploying Windows Server 2003 in mixed mode.

1. **Select multiple user objects.** Modify attributes of lots of user all in one go. This feature actually works like NT 4.0's User Manager. For a variety of reasons, multiple selection was not availably in W2K, which made it tedious to change several users home directory in one operation.
2. **Drag-and-drop ability.** One irritation of W2K is that you cannot drag and drop users and computers between OUs. This has been corrected in the latest Active Directory.
3. **Save your queries.** Tip: save search queries that you use often in Active Directory Users and Computers, it saves time when you have to repeat the query later.
4. **Application directory partitions.** Useful for controlling the replication scope for DNS (Domain Name System) data stored in Active Directory so that only specific domain controllers in the forest replicate DNS zone information.
5. **Universal group membership cached.** Avoid the need to locate a global catalog across a WAN link during logons, by storing user universal group memberships on an authenticating domain controller.

6 Features Available in Windows Server 2003 Level

A reminder that this highest level means all domain controllers are running Windows Server 2003 (No NT 4.0 BDCs or Windows 2000 DCs).

1. **Domain rename.** Rename any domain in the Windows Server 2003 forest. Now you can change the DNS name or NetBIOS name of any child domain or even the forest root domain.
2. **Domain controller rename tool.** Rename domain controllers without having to run DCPROMO and demote them.
3. **Forest trusts.** Create a two-way transitive trust to join two forests. Very useful for amalgamating companies.
4. **Replication enhancements.** Unnecessary traffic was created in W2K when you added one member to a group; it resulted in the whole group membership being replicated. Linked value replication allows individual users to be replicated instead of replicating the entire group membership.
5. **Global catalog replication.** Similar to the above, less traffic is replicated when changes are made to the Global catalog
6. **Defunct schema objects.** Deactivate classes or attributes from the schema which you know you will never use.

Raise FOREST Levels

1. All domains at Windows Server 2003 level.
2. At least one domain at Windows Server 2003 Interim, meaning some NT 4.0 domain controllers.
3. Windows 2000 level (default) mixture of NT 4.0, Windows 2000 levels.

Key extra features of a forest at Windows Server 2003 level

1. Cross forest trusts
2. Domain Rename (There are more advantages for schema developers)

What is new in Server 2003?

This section is practically all new. Windows 2000 just had mixed mode and native mode. Server 2003 expands the modes to having a third mode Server 2003 native. There is also a special mode for NT 4.0 and Server 2003 (No Windows 2000).

There was no concept of Forest level in Windows 2000.

Summary and Recommendations

1. Have you noticed how setting a date for an event creates extra power? Make targets for raising your domain and forest levels.
2. Make raising the domain level an opportunity to investigate new features in Server 2003.

7) Schema

The heart of Active Directory

Introduction to the Schema

The Schema Snap-in is not available by default. There lies a clue that ordinary administrators are not meant to change the Schema. However, to complete your understanding of Active Directory take time to appreciate the object model that underpins Windows Server 2003.

Topics for the Schema

What you need to know about the Schema.

Object based Nature

Studying the Schema will help you understand the object nature of Active directory. The schema keeps a list of the definitions for each object such as Computer or User. The list is divided into Classes and Attributes and the Schema recycles attributes like location and applies the same definition of location to the site, printer or computer object. For example, location will always be a text field, whereas Update Sequence Number will be a numeric field.

Flexible Master Role

The Schema master is one of the five single master roles, this means that only one domain controller has read and write access to the schema. Take the time to find out which machine holds the Schema Master role. Right Click the Schema Snap-in, select Operations Master from the short cut menu.

Modification by Exchange 2003 and Schema Admins

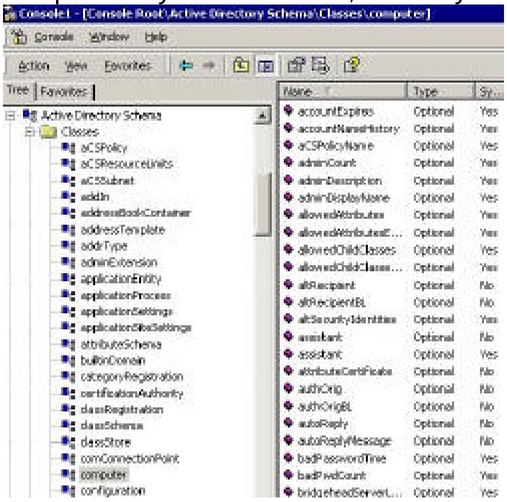
Exchange 2003 relies on Active Directory for definitions of the users mailboxes. When you install Exchange 2003, firstly, you have to be a member of the Schema Admin Global group; secondly, Exchange extends the schema to include extra attributes like mailbox server. While it is possible to add attributes and classes yourself - resist. Modifying the schema affects the entire forest and in my opinion should only be done by a developer when there is a clear business need.

Role of the Global Catalog

The Global Catalog server keeps track of a subset of the most important attributes, and the Global Catalog replicates this information to other Global Catalog servers. Be aware that you can add extra attributes to the replication list, for example, information on department could be replicated. The benefit is you could search on the department field to find a suitable user.

Getting Started

To make the Schema Snap-in appear, first you need to register a dll.: Start, Run, and regsvr32 schmmgmt.dll. Next, I add the Schema snap-in to my MMC. Run, MMC if you need to create a blank shell for the snap-ins, then its File (Menu) Add/Remove Snap-in.


Console1 - [Console Root\Active Directory Schema\Classes\computer]
Console
Window
Help
Action
View
Favorites
Tree
Favorites

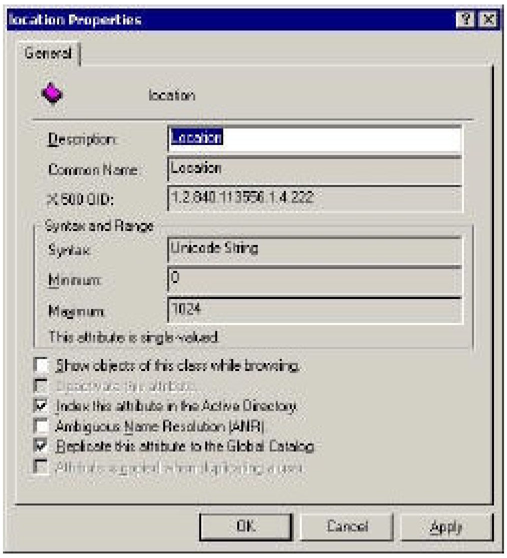
Active Directory Schema
Classes
aCSPolicy
aCSResourceLimits
aCSSubnet
addIn
addressBookContainer
addressTemplate
addrType
adminExtension
applicationEntity
applicationProcess
applicationSettings
applicationSiteSettings
attributeSchema
builtinDomain
categoryRegistration
certificationAuthority
classRegistration
classSchema
classStore
comConnectionPoint
computer
configuration

Name	Type	Sy...
accountExpires	Optional	Yes
accountNameHistory	Optional	Yes
aCSPolicyName	Optional	Yes
adminCount	Optional	Yes
adminDescription	Optional	Yes
adminDisplayName	Optional	Yes
allowedAttributes	Optional	Yes
allowedAttributesE...	Optional	Yes
allowedChildClasses	Optional	Yes
allowedChildClasse...	Optional	Yes
altRecipient	Optional	No
altRecipientBL	Optional	No
altSecurityIdentities	Optional	Yes
assistant	Optional	No
assistant	Optional	Yes
attributeCertificate	Optional	No
authOrig	Optional	No
authOrigBL	Optional	No
autoReply	Optional	No
autoReplyMessage	Optional	No
badPasswordTime	Optional	Yes
badPwdCount	Optional	Yes
bridgeheadServerL...	Optional	Yes

The schema shows all the objects that exist in Active Directory. Examples of Active Directory Schema Classes include: **computer**, printer and user

Each object has attributes e.g. CN = Common Name, Department, HomeDrive and USN. From a design point of view, Microsoft implement 'mix and match'. Once an attribute like Location is created, it can be matched with several objects e.g. Printer Object or Computer Object. Finally, attributes have values, which you set, through interfaces like the Active Directory Users and Computers.

While knowledge of the object-based systems builds a picture of Active Directory, there is practical value in understanding the role of the schema in Active Directory. For instance, when you install **Exchange** 2000 you need to be member of the Schema Admins otherwise your install will fail. You should also be aware that Exchange 2000 alters the schema so that 4 new Email tabs are added to users' property tabs.



location

Description: Location
Common Name: Location
X.500 OID: 1.2.840.113556.1.4.222

Syntax and Range
Syntax: Unicode String
Minimum: 0
Maximum: 1024
This attribute is single-valued

□ Show objects of this class while browsing.
□ Deactivate this attribute.
☑ Index this attribute in the Active Directory
□ Ambiguous Name Resolution (ANR)
☑ Replicate this attribute to the Global Catalog
□ Attribute is copied when duplicating a user

Inspecting the Schema Snap-in

Once you have registered the Active Directory Schema you can check out the Classes and Attributes; this will give you an idea of how objects like users are built up of attributes. Do not worry about the X500 OID, but do inspect the Attributes Properties to see which are published in the Global Catalog. The Global Catalog is a subset of the Schema containing the most useful attributes, which are used in the Search menus.

In my opinion, you should only create new Classes or even new Attributes if you are a developer. One extra Class I have heard suggested is Laptop. Personally, I think that there enough user attributes, but someone suggested adding a Car with an Expense attribute.

Where might you use this Schema Knowledge?

Understanding the objects and attributes is vital if you wish to use tools like CSVDE or LDIFDE to bulk import users. Alternatively, TechNet may guide you to make changes to LDAP properties using ADSI. Knowledge of the Schema properties will give you confidence to manipulate Active Directory objects using low-level utilities.

What's new in Server 2003

Deactivating attributes

Active directory will not allow you to delete classes or attributes but you can deactivate them if you are sure they will not be needed.

Improved replication

In Windows Server 2003, only changes in attributes are replicated, the benefit is less replication traffic and less change of a conflict.

ADPREP

Active Directory preparation allows you to extend the schema ready for an installation of the NTDS.dit database files. ADPREP uses /forestprep and /domainprep switches rather like Exchange 2000/3.

Summary and Recommendations

1. Take the time to understand what the schema does for Active Directory.
2. Register the Schema snap-in.
3. Find out which machine has the Schema Master Role.
4. Normally you will not need to alter the schema itself. The only time the Schema is extended is when you install Active Directory aware programs like Exchange 2003.
5. Knowledge of the Schema is helpful when you need to use ADSI or CSVDE.

8) FSMO

Here are five roles, which can only be held by one Domain Controller

Introduction to FSMO (Flexible Single Master Operations)

There are two reasons for investigating FSMO.

a) Curiosity: To know how these single master operations works.

b) Planning: To know what to do if you lose one of these 5 FSMO roles.

Topics for FSMO

Background information

For most Active Directory operations, Windows 2003 uses the multiple master model. The benefit of the multiple master system is that you can add a computer, or change a user's password on any domain controller. For example, if you have three domain controllers, you can physically create a new computer in the NTDS.dit database on any of the three. Fifteen seconds later, the new computer object will be replicated to the other two domain controllers.

Technically, the multiple master model uses a change notification mechanism. Occasionally problems arise with duplicate operations, and as a result, orphaned objects appear in the 'LostAndFound' folder. The point of FSMO is that a few operations are deemed so critical that only **one** domain controller can carry out that process. Emulating a PDC is the most famous example of a Single Master Operation; creating a new child domain would be another example of a FSMO role.

In FSMO, F means Flexible. In practice, this means that you can move any of the five roles to a more suitable domain controller.

The five FSMO roles are:

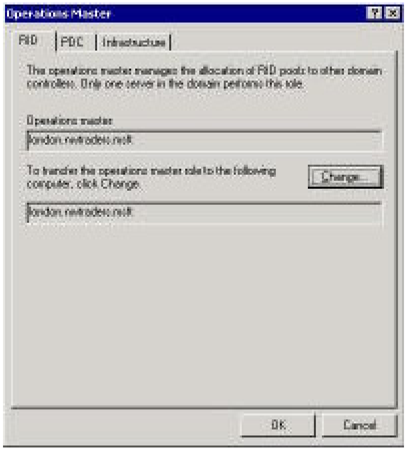
1. PDC Emulator - For NT 4.0 BDC's. But also for synchronizing time and creating group policies.
2. RID Master - Each object must have a globally unique number. The RID master makes sure each domain controller issues unique numbers when you create objects like users.
3. Infrastructure Master - Responsible for checking Universal group membership in multiple domain forests.
4. Domain Naming Master - Ensures that each child domain has a unique name.
5. Schema Master - Operations that involve expanding user properties e.g.
6. Exchange 2000 adds the mailbox property to users.

   Three of the FSMO roles (1-3) are held in each domain, whilst two (4-5) are unique to the entire forest.

Changing the FSMO roles

RID, PDC, Infrastructure (1. 2. and 3.)

You can plan a switch of Operation Master by using the Change button in the diagram right, taken from Active Directory Users and Computers, Right Click Domain, Properties, **Operations Masters.**



This operations master manages the allocation of RID pools to other domain controllers. Only one server in the domain performs this role.

Operations master:
london.reviradero.nsft

To transfer the operations master role to the following computer, click Change.

london.reviradero.nsft

Domain Naming Master (4.)

To see the Domain Naming Master (4), check out Active Directory Domains and Trusts, Operations Master...

Schema Master (5.)

The Schema Master (5) is the most difficult FSMO to find.

1) Register the Schema Snap with this command: RUN *regsvr32 schmmgmt.dll;*

2) Run MMC, Add Remove Snap-in, Add Active Directory Schema

3) Select Active Directory Schema, Right Click, Operations Master.

If you ever run DCPROMO to demote a domain controller, watch out for a check box that says 'This is the last domain controller in the domain'. If that box is UN-checked, the wizard will automatically move any FSMO roles to another domain controller.

What to do when you lose a FSMO machine

Firstly, do not rush to replace a FSMO domain controller. Strange advice you may think, but my point is that Active Directory should be able to work for a few hours without the FSMO machine. The frustration would be if you transferred the role, only for the original machine to return, then the two machines with the same FSMO role would 'fight' and so cause you more problems. To resolve the matter you would have to reformat the partition with the operating system on the original machine - then rebuild.

FSMO (Flexible Single Master Operations)

If you lose one of the FSMO roles, you have to decide whether to 'seize' the role onto another Domain controller, or wait for the original machine to be brought back into service. Each role and each circumstance needs careful consideration so take the time to understand the implications of your actions.

1. **PDC Emulator**
2. **Infrastructure Master**
3. **RID Master**
4. **Schema Master**
5. **Domain Naming Master**

PDC Emulator

Of the five roles, this is the role that you will miss the soonest. Not only will any NT 4.0 BDC's complain, but also there will be no time synchronization. Another problem is that you probably will not be able to administer group policies as the PDC emulator is by default, the group policy master.

Implications for Duplicates

If the old PDC emulator returns, then the situation it not as serious as with duplicates of some of the other roles. The answer is to seize the PDC role from the old machine on to the new machine.

Recommendation

The way to change the role when you lose a FSMO Master, is to use NTDSUTIL. This built-in utility runs from the command line. Type NTDSUTIL, Roles, Help, Connect to server %, Seize PDC.

TIP Make plenty of use of HELP. Get into the rhythm of the command.

Infrastructure Master

The consequence for a missing Infrastructure master is that group memberships may be incomplete. If you only have one domain, then there will be no impact, as the Infrastructure Master is responsible for updating your user's membership in other domains in the forest.

Implications for Duplicates

No damage occurs if the old Infrastructure master returns, just check out the Roles and decide which machine should hold the role.

If you must seize the role then check out the NTDSUTIL **Recommendation**

RID Master

Only one Domain Controller is responsible for allocating a pack of unique numbers to the other domain controllers, this Single Master Operation ensures that no two new objects have the same GUID (Globally Unique Identifier).

If you lose the RID master, the chances are good that the existing Domain Controllers will have enough unused RIDs to last a week or so, therefore, do not be in a hurry to seize the RID master onto another machine. Seize in this context means create a new RID master.

Implications for Duplicates

You must not allow two RID masters to appear in the same domain; if you did, there is the possibility of two objects having the same RID, which would be disastrous for security. Therefore, if the original is found, it must be reformatted and reinstalled before re-joining the domain.

If you must seize the role then check out the NTDSUTIL **Recommendation**

Schema Master

Remember that you can only have one Schema Master in the entire forest. Usually this role is allocated to one of the domain controllers in the root domain. If ever you had two Schema Masters you risk splitting the forest, which would lead to instability. The good news is that once the forest is created and Exchange is installed, there is little need for the Schema master. So wait until there is no chance of repair or return of the first Schema master before you consider seizing the role.

Domain Naming Master

The only time that you need this role is when you are creating child domains. As with the Schema master, firstly wait until you are sure the first one has disappeared for good, secondly do not allow two Domain Naming Masters to exist anywhere in the forest.

What's new in Server 2003

I have not been able to find anything new regarding FSMO, it works just the same in Server 2003 as it works in Windows 2000.

Summary and Recommendations

1. Record not only where the FSMO roles are now, but also identify a standby machine in case of failure.
2. If a FSMO machine is down, evaluate the effect and decide how long you have before you need to seize the role to another domain controller.
3. Master NTDSUTIL so that you can replace the FSMO role from the command line.

9) Physical Sites

The other side of Active Directory

Introduction to Sites - The physical side of Active Directory

Even seasoned professionals sometimes forget that physical sites are completely separate from the logical structure of your domains and trees.   It makes sense to have one domain spread over several sites, but it is also possible to have one site with domain controllers from different domains. If you are familiar with Exchange Sites, then the principles are the same in Active Directory.

Topics for Physical Sites

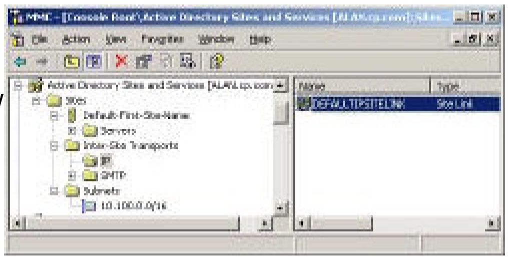
1. Strategy for Creating Sites
2. Configuration of Sites
3. What's new in Server 2003 Sites
4. Summary and Recommendations

Strategy for creating Sites

The main reason for creating another site is to control directory replication. Active Directory exploits multiple master replication. Unlike NT 4.0, with Active Directory you can create new users and computers on any domain controller. If all servers have fast links, then you can keep all domain controllers in the same site and replication will happen automatically every 15 seconds.

Where connections between servers are physically slow, create a new site and regulate the time that connectors are open for replication traffic. Speed is a relative term and 28K links would indicate separate sites, where as T1 or E1 links would mean that servers can operate in the same site. If you are in doubt, consider running System Monitor to check for a bottleneck.

Configuration of Sites



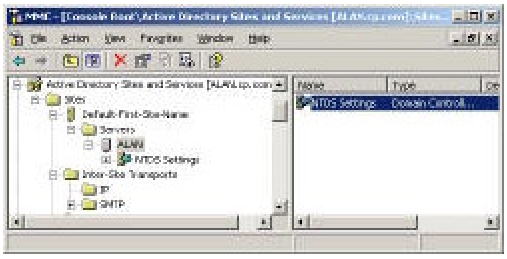
Setting up a new site is a job for the Active Directory **Sites and Services** and creating a new site. Initially all the Domain Controllers are in the Default-First-Name-Site; what you should do is add more sites and create Subnets to reflect the TCP/IP network. Then move the servers to their relevant sites.

Subnet

Each site will consist of one or more subnets. When you configure sites, you also need to associate subnets with sites. Remember to fill in the Location attribute of both the site and the subnet so that users will be able to 'find a printer near me'.

Site Links

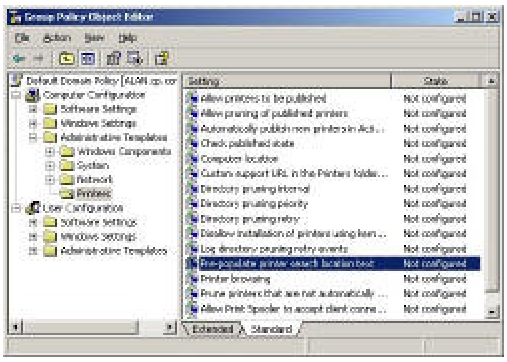
Unlike LAN replication traffic, replication packets between sites are compressed to about 15% of their former size. Configuring the Site Links is a matter of deciding the time of day, and frequency, which sites replicate Active Directory traffic. Favour a fully routed network, and avoid Site Link Bridges if possible.


MMC - [Console Root\Active Directory Sites and Services [ALAN.cp.com]\Site...
File Action View Favorites Window Help
Active Directory Sites and Services [ALAN.cp.com
Sites
Default-First-Site-Name
Servers
ALAN
NTDS Settings
Inter-Site Transports
IP
SMTP
Name
Type
NTDS Settings
Domain Controll...

There are lots of sub menu within the Active Directory Sites and Services snap-in. Be aware that the server object in the Sites has separate configuration settings from the server object in Active Directory Users and Computers. It is worth exploring the NTDS Settings properties, see middle diagram.

Location Attribute

TIP Take the time to match the Location attributes. Check the Location attribute on each of these three places: Site, Subnet and Printer. My point: make sure that the value for the Location set on the Subnet and Site objects matches the Printer Location.



Setting	State
Allow printers to be published	Not configured
Allow pruning of published printers	Not configured
Automatically publish new printers in Acti...	Not configured
Check published state	Not configured
Computer location	Not configured
Custom support URL in the Printers folder...	Not configured
Directory pruning interval	Not configured
Directory pruning priority	Not configured
Directory pruning retry	Not configured
Disallow installation of printers using kern...	Not configured
Log directory pruning retry events	Not configured
Pre-populate printer search location text	Not configured
Printer browsing	Not configured
Prune printers that are not automatically ...	Not configured
Allow Print Spooler to accept client conne...	Not configured

The final piece of the Printer Locations jigsaw is to set a policy in Active Directory that sets the location when users search for a printer. Here is the Group Policy reference: Computer Configuration - Administrative Tools - Printers - See Diagram opposite.

Now you are ready to test by Searching for 'Printer on the Network'.

What's new in Server 2003 Sites and Subnets

Under the covers, replication now takes place at the attribute level. This has twin benefits, less traffic and less conflicts because two administrators can now simultaneously change different attributes on the same object.

Summary and Recommendations

1. Configure the Subnet Object with IP addresses that match your physical network.
2. Schedule Active Directory traffic for off peak times.
3. Use fully linked networks rather than site linked bridges.
4. Master the Location attribute settings for Printers, Subnets, Sites and Group Policy.

10) Migration to Server 2003

Plan your move to Server 2003 Active Directory

Introduction to migrating to Server 2003

There are three possible strategies for a successful transfer from an NT 4.0 domain to Active Directory. My goal is to give you the information so that you can decide which strategy will be right for you.

1. Migrate to a 'Brand New' Windows Server 2003 domain.
2. 'In Place' upgrade from NT 4.0 to 2003.
3. Co-existence of NT 4.0 with Windows Server 2003.

Topics for migrating to Server 2003.

Migration Strategies

1. Brand New Domain

Faced with moving to Windows Server 2003, my first choice would be to create a 'Brand New' domain. There are many advantages of a clean start. For instance, you may want to change your NT 4.0 domain name to match your DNS name. Also, you probably want to ditch all that baggage from your old domain.

The hardest part of this strategy is to deal with the user accounts. Two common solutions are to:

a) Export the old accounts in NT 4.0, then use CSVDE to bulk import into Active Directory.

b) Get ADMT and move the accounts from NT 4.0 into the new domain.

2. 'In Place upgrade from NT 4.0.

The simplest strategy is to make an 'In Place' upgrade of NT 4.0. Just insert the CD for Windows Server 2003 into the NT4.0 PDC and the wizard will guide you through the upgrade. Then repeat this procedure for each of your BDCs. In my opinion, this 'In Place' method is only suitable for small networks with 10-150 users. In its purest form, this strategy means finishing on Friday as NT 4.0 and coming in on Monday upgraded to a Windows Server 2003 domain.

One worry with the 'In Place' migration is that there is no easy rollback should things go wrong. One tactic is to keep a BDC available but off the main network. If there is a problem, with the migration bring this BDC back and promote it. Meanwhile while you rebuild the previous PDC offline then try the migration once again. Alternatively, you could restore from that backup you made before attempting the upgrade.

3. Co-existence of NT 4.0 with Windows Server 2003.

Co-existence would be my last choice. While it is true that co-existence is the most versatile strategy, it does mean extra work running both NT 4.0 and Windows Server 2003. If you are not careful, the users become confused, and this would make them hostile to the upgrade - which would be a shame.

I accept that for large organizations, co-existence may be the only practical solution. At its simplest, it could mean an extension of the 'In Place' strategy by upgrading a few NT 4.0 BDC's each month until the whole organization is native Windows Server 2003.

You could also use Co-existence in conjunction with my first strategy 'Brand New Domain'. Create a new Windows Server 2003 forest, and then configure trust relationships to the old domain. Where you need to preserve settings, Microsoft provide good tools to help you move users and their settings across to the new domain, e.g. ADMT and USMT.

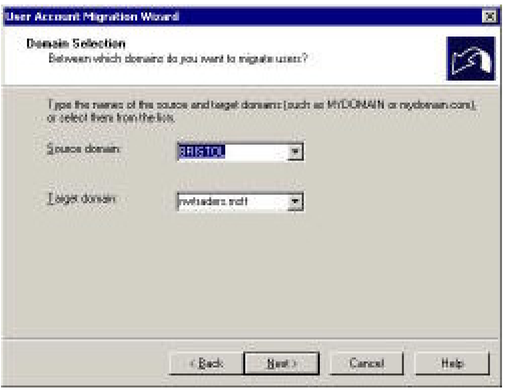
At this stage, it is important to reach a preliminary conclusion. Decide which strategy you are going to deploy, then read these pages to test and refine your Windows 2003 plans.

Two great utilities to help migrate client settings ADMT and USMT

ADMT v 2.0 (Active Directory Migration Tool)

This is a great tool for copying user account information from an NT 4.0 domain into a different domain in Windows 2003. The crucial attribute is the sIDHistory, this enables the user object to be identified in the old and new domain. The prerequisite for using ADMT is that the Windows 2003 domain has to be in Native mode.

You will also need to create a trust so that the NT 4.0 accounts domain trusts the Windows 2003 domain. As a result, the old accounts can be copied across to their new domain. Let me just clarify that the ADMT copies, it does not moves the accounts. Moreover, this is a one-time move without any synchronization. Should you need account synchronization then deploy the ADC (Active Directory Connector)



User Account Migration Wizard

Domain Selection

Between which domains do you want to migrate users?

Type the names of the source and target domains (such as MYDOMAIN or mydomain.com), or select them from the lists.

Source domain: BRISTOL

Target domain: nwtraders.msft

Note: You will find ADMT in the \i386 folder on the server CD.

User State Migration Tool

The User State Migration Tool (USMT) copies user settings, files, and documents. Then you restore these settings on the new machine so users do not have to reconfigure their desktop settings. It works best for XP and Windows 2000 Professional clients and you do need the client machine to be connected to a domain controller.

There are two command line utilities scanstate and loadstate that control the procedure.

Files and Settings Transfer Wizard

This wizard found on the XP CD includes the same functionality as USMT but does not allow for the fine-tuning of the settings that you get with scanstate and loadstate.

A fresh look at migration

With learning the benefits and pitfalls of a new product, you need to revisit the key concepts several times before making a decision. Here is a fresh look at your upgrade strategy.

Where are you now?

My first suggestion is to take stock and ask, 'Where are we now? Exactly what are our servers running?' The answers should be easy, we are running NT 4.0 or W2K. However, digging a little deeper, do you know which service packs are installed, the amount of RAM each server has, and the size of the system partitions? All this is leading up to my key question, 'Will the old machines run the new Server 2003 operating system?' Also, check the HCL (Hardware Compatibility List) on Microsoft's website. If you were still in doubt, I would download Microsoft's free compatibility testing software and prove that your system will upgrade successfully.

What is your Vision?

Now it is time to clarify, 'Where do you want to get to?' This is a deceptive question. The answer may not be as simple as migrating to Windows Server 2003. Perhaps you could use the migration as an opportunity to restructure your domains and consolidate on fewer, bigger servers? (Revise that budget figure and add extra money for new kit).

What I am driving at is develop a vision for IT in your organization. Imagine the best desktop for your user, think what services they need. Use migration as an opportunity to reduce costs, increase productivity. Windows server 2003 is a good choice to turn your vision into reality. But wait a minute, which 'flavour' of Server 2003 do you want? Enterprise, Web or Standard Windows 2003 server?

What's new in Server 2003

There are extra complications because there are now potentially three operating systems, not two. Server 2003 could integrate with NT4.0, and or Windows 2000. The big changes are the Raise Domain Settings, minor changes are improvements to ADMT and the sIDHistory attribute for migration from different domains.

Summary and Recommendations

Which of these routes will you take?

1. **Migration path NT 4.0 --> Windows Server 2003 (Recommended)**
2. Migration path NT 4.0 --> Windows Server 2000 (Consider above option)
3. Migration path W2K --> Windows Server 2003 (Easy, but would it be cost effective?)

Related Topics

1. **DNS**
2. **Installation**
3. **Raise Domain Level**

11) New Features for Server 2003

Check what has changed from Windows 2000

New Features in Server 2003

1. Logical
2. Group Policy
3. DNS
4. Install
5. Raise Domain Level
6. Schema
7. Physical Sites

Logical Structure

Forest Trusts. You can create trusts between forests

Once you Raise the Forest Level to Server 2003, then you can rename domain controllers or even the domains themselves.

DNS

All the major changes like Dynamic DNS and Active directory integration happened between NT 4.0 and Windows 2000. In Server 2003, the changes amount to tidying the menus and interfaces in the DNS Server object. For example, the Event Viewer is now under the server to remind you to check for DNS errors; Cached Lookups are visible without having to select advanced objects.

Install

ADPREP

Here is a built-in command line tool that will prepare the schema. It does not actually install the NTDS.dit files but it does prepare the forest or the individual domain for Active Directory.

ADPREP /forestprep

ADPREP /domainprep

DCPROMO /adv

If you already have a working domain controller, backup the system state, go to a member server, run DCPROMO /adv then point the wizard to the backup files

Group Policy

This Group Policy Management Consol is one of the best new features in the whole of Window Server 2003, it gives you complete control over all policy settings. The GPMC transforms management of policies. The only surprise is that you have to get a copy from Microsoft's Site, and that it is not available on the Server CD.

As well as the new interface there are 150 new Group Policies in Server 2000; these are in addition to the 250 new policies for XP compared with Windows 2000 professional.

One of the most common problems when testing group policy is they do not work as you expected. If nothing at all happens, the number one reason is the User or Computer is not in the OU with the policy! The number two reason is you just need to refresh the policy, here is the simple command - GPUpdate.

Schema

Deactivating attributes

Active directory will not allow you to delete classes or attributes but you can deactivate them if you are sure they will not be needed.

Improved replication

In Windows Server 2003, only changes in attributes are replicated, the benefit is less replication traffic and less change of a conflict.

Raise Domain Level

There are extra complications because there are now potentially three operating systems, not two. Server 2003 could integrate with NT4.0, and or Windows 2000. The big changes are the Raise Domain Settings, minor changes are improvements to ADMT and the sIDHistory attribute for migration from different domains.

Physical Site

Using the control or shift key to select and change one attribute in many users. (You could do this in NT, but not Windows 2000)

Under the covers, replication takes place at the attribute level. This has twin benefits, less traffic and less conflicts because two administrators can now simultaneously change different attributes on the same object.

12) Tools for Server 2003

Check out your Windows Server 2003 tool kit.

Windows Server 2003 Tools

(DC) = Only found on Domain Controllers

1. **ADMT** - Active Directory Migration Tool v 2.0
2. **ADPREP** - Active Directory Preparation
3. ADSI (DC) - Editor for Active Directory
4. ADSizer - Estimate hardware needed:
   microsoft.com/windows2000/downloads/tools/sizer/default.asp
5. CACLS - Set Permissions
6. **DCPROMO** (DC) - Promote your member server
7. **GPMC** - Group Policy Management Consol (Microsoft's web site)
8. MoveTree - Resource Kit migration tool
9. MMC - Microsoft Management Console
10. NETDiag - Troubleshoot network connections
11. **NTDSUTIL** (DC) - Troubleshoot DNS
12. REGSVC- Example Register the Schema Snap-in
13. REPLMON (DC) - Synchronize domain controllers
14. Resource Kit e.g. CMDHere, ADSI
15. RUNAS (Shift and Right Click an Administrative Tool)
16. SetupMgr - Creates Answer Files for installations **Schema** Snap-in (DC). **Run regsvr32 schmmgmt.dll,** the Active Directory Schema snap-in will now available in the MMC or Administrative programs
17. SIGVERIF - Check Driver Signing
18. **USMT** - User state migration tool
19. VISIO - Extra program you need to buy. Useful for designing your Active Directory forest.

Index of Windows Server 2003 Active Directory