Moving from Windows NT to Windows Server 2003

Jonathan Hassell provides a practical guide to making the big move

Many companies are finding themselves jumping the sinking Windows NT ship and considering an upgrade to the latest server product from Microsoft, Windows Server 2003. After all, the end-of-life date for the NT Workstation product was in mid-2003 and NT Server's death is fast approaching as well, so it's very possible that your organisation has some machines running NT that are worth upgrading.

Microsoft released Windows Server 2003 in late April 2003, and since then it has matured via various updates into a server product that, in my experience, is more stable, reliable and secure than any previous version of Windows. There's an upcoming service pack that should ship in the middle of this year, which is usually the 'flag' date when companies really consider upgrading to the newest Microsoft operating system. So this is an excellent time to consider upgrading.

ITEMS TO CONSIDER BEFORE MIGRATING

If you currently have an NT domain and haven't yet investigated AD (Active Directory), the directory service that Microsoft first introduced in Windows 2000 Server, there's a lot in store for you. AD is superior to NT-style domains in many ways, not least of which is easier management.

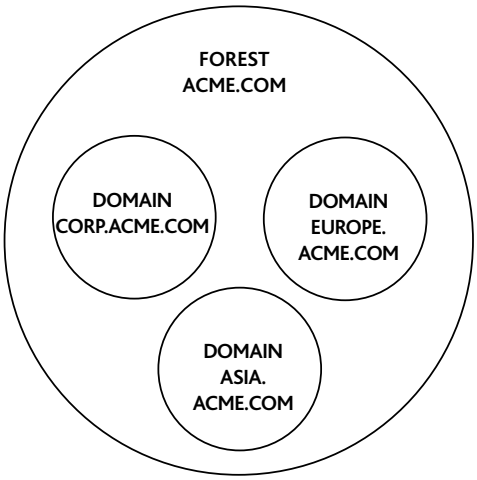


Figure 1. How Active Directory forests, domains and trees fit together.

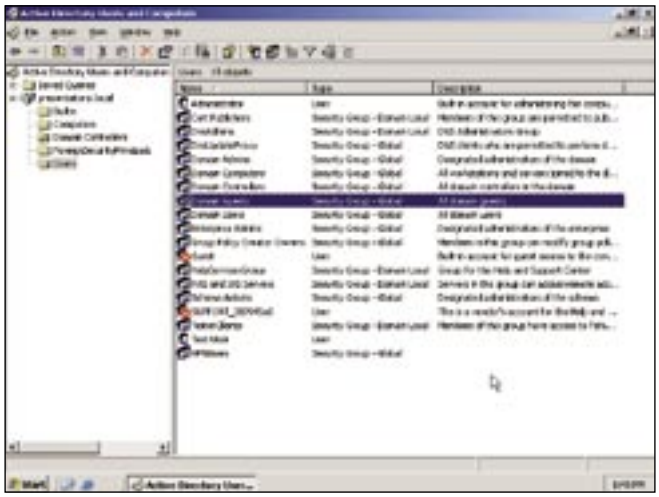


Figure 2. Active Directory Users and Computers, the standard tool to manage objects within the directory.

You can divide your directory into specific domains and organisational units and manage like sets of objects with ease. AD is more robust and fits better into more distributed environments, particularly in organisations with branch offices in multiple locations. AD is more secure for your users and is also the foundation of many newer versions of Microsoft server products, including Exchange Server 2003.

AD allows you to create forests of objects, inside which you place domain trees that can contain within them organisational units (OUs). Objects can be placed within the domain trees under any number of scenarios – you may want separate OUs for computers and user accounts, or different OUs per departments, or any other management strategy. You can also use Group Policy to create a structured, consistent environment among all the objects within the directory. It's a wonderful upgrade from regular NT domains, but the added functionality certainly makes for a more complicated upgrade. See Figure 1 for an example AD structure, and Figure 2 for a screenshot of AD Users and Computers, the management tool for AD administrators.

There are several different steps in moving from NT to Windows Server 2003 and AD. First, you'll want to analyse your current NT domain environment. Specifically, find answers to these questions:

- *Are you on a single domain or multiple domain model, with accounts and computers located in each domain, or do you have a single master or multi-master domain model, with separate domains each for user accounts and machine resources?*

The single domain model is the easiest to upgrade, since the existing domain simply becomes the root of the AD domain. However, if you have a particularly large domain or a network that might be restructured one day, then you may want to consider a dedicated forest root model (sometimes called an empty root), in which you create a root domain within a forest and then create child domains off of that root. This allows you to change domains in the forest without scrapping your entire AD structure. If you have a single master domain and child domains containing machines, you really don't need to continue that structure upon moving to AD, since you can create OUs to store specific types of objects within the directory. Multiple masters will want to use the dedicated forest root strategy, since complex networks should still be broken up by domains, even in AD, for easier management.

- *What sort of trust relationships have you built up with other domains in your environment?*

Trust relationships can make moving to AD more complicated, but they don't have to be difficult.

Next month: Migrating from Windows 2000 to Windows Server 2003

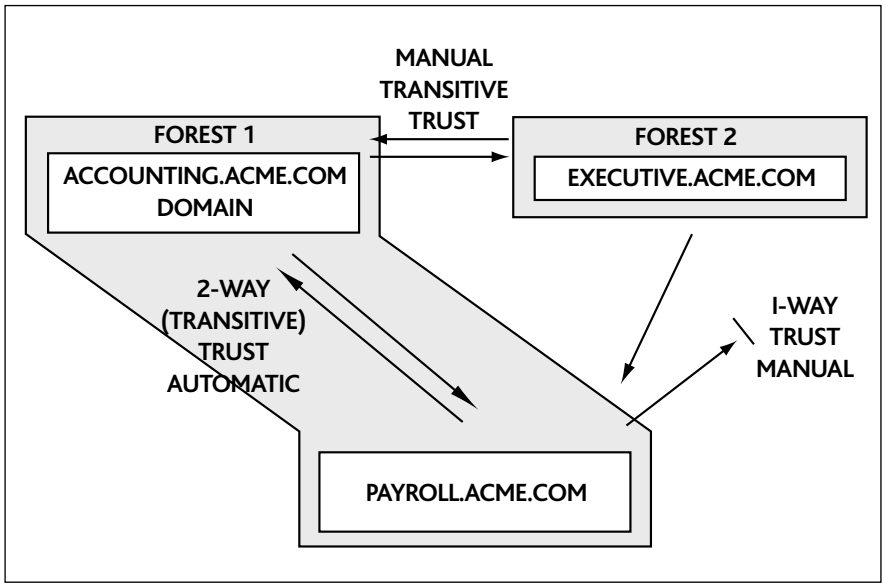


Figure 3. How trust relationships can be created and used within AD.

If you have trusts among a multi-master domain model, in that every domain trusts every other domain, you need do nothing if you put all of these domains into a single forest – all of these trusts between domains are automatically transitive. If you have one-way trusts that you want to preserve for logistical reasons, you'll need to create multiple forests, which can be a headache; make sure this is the route you'd like to take before doing so. Figure 3 shows some sample trust relationships in AD and how they fit together.

● *How many primary domain controllers (PDCs) and backup domain controllers (BDCs) do you have, and where are they located – all in one location, or at separate sites?*
In AD, there are really no distinctions between PDCs and BDCs (with a couple of minor exceptions). Plus, Windows Server 2003 is more robust than NT 4, so you can likely consolidate multiple domain controllers at a single location into a smaller number, depending on their load. Your main concern with domain controllers is their location. Part of AD's technology is a replication algorithm that sends updated contents of the directory to all domain controllers within the forest, even at different sites. If you have offices in different locations with slow links, which you can define within AD, this will affect your replication speed and how quickly those users at the remote offices can get authenticated and receive access to domain or forest resources. You'll want to look at how these locations will play into where you allocate domain controllers. Figure 4 shows how sites and replication works within a sample company's AD structure.

If you have offices in different locations with slow links, which you can define within AD, this will affect your replication speed

● *If you have DNS deployed internally, what namespaces are you using and how are they assigned?*
You'll want to catalogue all of these internal domain namespaces and decide how they 'map' into your new AD structure. Particularly of note are how you may want DNS subdomains (for example, corp.acme.com) to map to actual AD domains in a forest and if you'd like to have external DNS services separated from internal DNS services. Of course, DNS is a major component of AD and entire books are written about planning and using DNS in AD environments, so be sure to read up on best practices or bring in someone experienced in DNS planning to assist you in your migration efforts.

● *Do you have any NT 4 servers that are running the Routing and Remote Access Service (RRAS) or the LAN Manager Replication Service?*
The NT RAS machines, be they domain controllers or just ordinary member servers, really don't integrate well within an AD environment. If you have a member server functioning as a RAS machine, you should upgrade it to Windows Server 2003 before the last domain controller is upgraded. The RAS machine has certain security requirements that are incompatible between the different operating system versions. This also is to say that if you only have one DC in your domain, you need to upgrade your RAS server before beginning any DC upgrades. Also, the LAN Manager Replication Service is incompatible with the new File Replication Service found in AD, so disable that as well.

● *Do you have any machines running versions of NT earlier than 4?*
You really need to rid yourself of these machines, as they're just incompatible with both Windows Server 2003 and an AD environment.

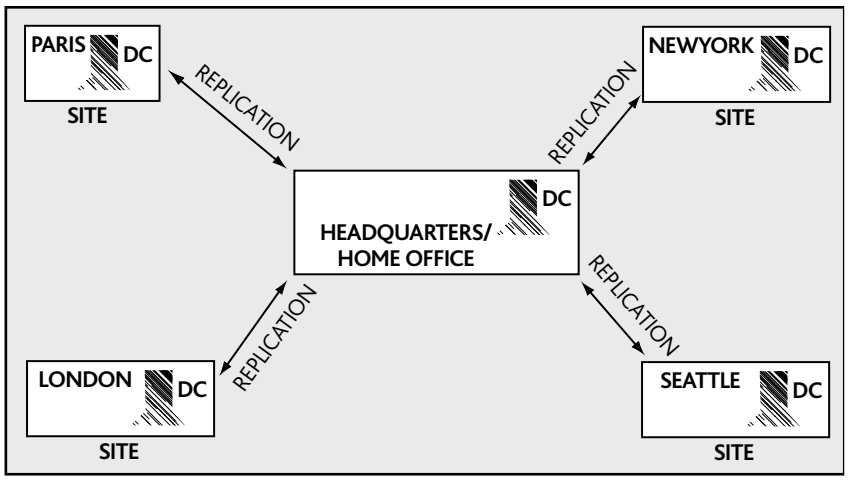


Figure 4. Denoting branch offices as sites with Active Directory to control replication traffic.

MIGRATION STRATEGIES

Any migration process is risky, since your environment is changing. In this section, we'll take a look at some prudent strategies to mitigate that risk and ensure that the entire move from NT domains to Windows Server 2003 and AD will go smoothly.

First, make sure that for all NT domains you're touching with the migration, you have at least an up-to-date BDC as well as the PDC. If the PDC for some reason fails to upgrade, then the BDC can be promoted to PDC and nothing is lost but some time. If you have two BDCs, the best strategy is to leave one online during the migration, so users more or less don't notice

anything is going on, and take the other offline during the upgrade. This way, the offline BDC isn't touched by anything happening during the upgrade and can be plugged in should everything go haywire. Figure 5 shows this procedure.

Also, synchronise your BDCs with their partner PDCs before proceeding. Out-of-date replication partners don't help anything when it comes to restoring service in the event of an outage. In the course of the migration, be sure to keep track of any changes you make after you take your BDCs offline – if your migration fails and you promote your BDC to a PDC, you'll lose any changes you made since you took the BDC offline, and you'll need to manually redo any changes you made in that period.

Take some time to look specifically at the PDC for each domain and figure out if it's sufficiently powerful. When we said earlier that there are virtually no distinctions between domain controllers anymore, there are a couple of exceptions – the first domain controller upgraded into AD will take on some roles that others don't have that will require a bit more operational horsepower.

If you're in doubt as to whether your PDC is powerful enough, a common suggestion is to buy a new machine and load it with NT 4 and Service Pack 6 and configure it as a BDC. Then, promote it to a PDC and put it on the network for a while to let the changes settle out and replication to finish. Then, take it offline and upgrade the machine to Windows Server 2003. This is the nearest strategy to a clean install and usually gives you the best results. If you have more than one domain, do this for each domain. (Do note that if you decide to use the dedicated forest root strategy, you'll need to have a native Windows Server 2003 machine with AD and create the forest and root domain first before upgrading any PDCs.)

PERFORMING THE MOVE

It's remarkably easy to upgrade any type of Windows NT installation, whether a PDC, BDC, or a regular member server, to Windows Server 2003. Microsoft has taken great pains to ensure the upgrade to Windows Server 2003 is as painless as possible. The installation procedure follows a normal clean install of Windows Server 2003 reasonably closely, and in fact requires less hands-on work. The program doesn't prompt you at all after the inception of the installation; there's little to no reconfiguration required with an upgrade installation, since existing users, settings, groups, rights and permissions are saved and automatically applied during the upgrade process. You also don't need to remove files or reinstall applications with an operating system version upgrade. So at the beginning, you're only asked for the CD Key and to acknowledge any compatibility issues, and then some time later the upgrade is complete. There are, however, a few points of which to take note:

Figure 6. Using the Check Upgrade function of Windows Server 2003's setup to look for issues to correct.

● *Service pack levels*

The Windows NT installation must be running Service Pack 5 or later. The most recent update, Service Pack 6a, can be downloaded from **www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.asp**. Other acceptable Windows NT versions include NT Terminal Server Edition with SP 5 or later, and NT Server Enterprise Edition, also with SP 5 or later.

● *Evaluating immediate setup issues*

On a machine that's a candidate for Windows Server 2003, insert the Windows Server 2003 CD and run WINNT32.EXE with the /checkupgradeonly switch. This will present a report to you with issues that the Setup program detects may cause problems with an upgrade to Windows Server 2003. Figure 6 shows a sample report.

There are also some disk issues regarding storage that you may want to examine before upgrading.

● *Partition sizes*

On machines upgrading from NT to Windows Server 2003, ensure there's plenty of disk space on the system partition of each machine. This is especially true of domain controllers, since converting a SAM database to an AD database full of the latter's capabilities can increase the size of the SAM by as much as ten times.

● *File systems*

Domain controllers require their system partitions to be formatted with the NTFS file system. While as a general procedure we recommend formatting all partitions on all server machines with NTFS, you aren't required to do so unless the machine in question is a domain controller.

● *Volume, mirror, and stripe sets*

Upgrading to Windows Server 2003 Enterprise Edition from NT on a system with volume, mirror or stripe sets (including stripe sets with parity) that were created under NT requires some modifications of those sets. Since Windows Server 2003 includes new dynamic disk technologies, support for older enhanced disk features has been removed – and this is indeed a change from Windows 2000. You'll need to break any mirror sets or, for all other media sets, back up any data on the set, and then delete the set. When Setup is complete, you can then replicate your existing disk configuration using native Windows Server 2003 tools and restore any data required from the backups.

MOVING DOMAINS TO ACTIVE DIRECTORY

The upgrade procedure for an NT domain is relatively straightforward. You must initially choose the first server to upgrade in your Windows NT domain. As you upgrade different machines, depending on their existing role in the domain, features and capabilities become available with Windows Server 2003 on the upgraded machine. In particular, upgrading an NT PDC enables all the included AD features, as well as the other capabilities inherent in any Windows Server 2003 server, such as improved routing and remote access service features, no matter the role. Note that you can upgrade Windows NT member servers at any time during your migration plan, and most migration plans specify that member servers are last on the list

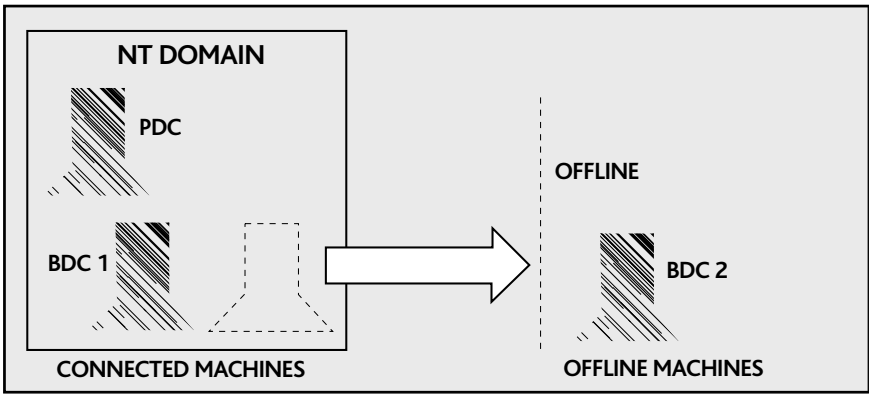
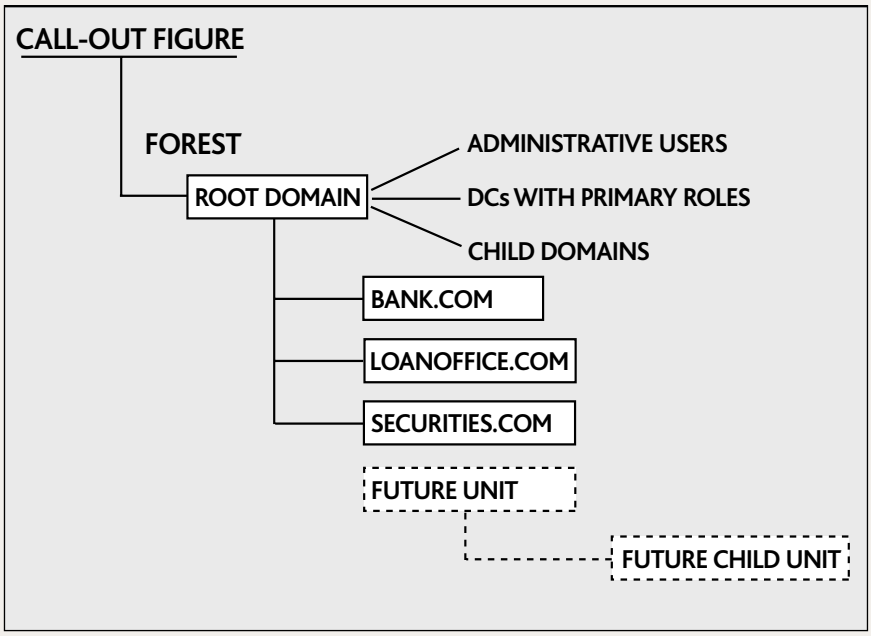


Figure 5. Taking a synchronised BDC offline as a failure recovery strategy.

THE DEDICATED FOREST ROOT MODEL

The dedicated forest root model provides a way to maintain the autonomy of multiple NT domains that you may have. This diagram shows how this is achieved.

A dedicated forest root domain can be either an 'empty domain', which only contains a small number of universal users and resources, or a normal production domain that just happens to be at the root of a forest. The latter isn't recommended. There are several advantages to having an empty forest root domain that does *not* serve as a production domain. For one, the domain administrators group in the root domain has power over the forest, which is something you may not want. Keeping the root empty allows you to delegate administrative authority to individual domains without giving everything away. It also helps you to structure your AD environment; a constant root makes further changes – for instance, if you acquire a new company or build a new office – logical and easy to implement and manage. The forest root domain, if kept empty, is very easy to replicate and to back up. And if changes to the administrative authority in your business ever are made, you can transfer the keys to the kingdom to others without affecting the administrators' autonomy of your child domains.



How the dedicated forest root model enables separate NT domains to be separate in AD.

All in all, the forest root domain is a good model to keep existing NT domains separate, and should be kept free of production objects that are best left to child domains.

to receive the upgrade. However, no matter your order, when you begin upgrading NT domain controllers to Windows Server 2003, you must upgrade the PDC before any other DC machines.

Here's a checklist of some steps to take immediately prior to your move to ensure your NT to Server 2003 migration goes smoothly:

- Make sure that all PDCs and BDCs are running Windows NT 4 with at least SP 5 or SP 6a.

- Clean up your domain account list, both for users and computers. We all know these lists can be cluttered with inactive users, multiple accounts for the same user, and so on. Take this opportunity to eliminate excess baggage from your directories before moving these objects into AD.

- Remove any unused software via its uninstallation facility, and defragment the hard disk to take advantage of any unused space. AD migrations can use a lot of disk space – sometimes upwards of ten times the size of the SAM database for an NT domain – and contiguous free areas of the disk can speed AD query response time.

- Kill any trusts between domains that you don't want preserved over the migration. DCs in Windows Server 2003 by default digitally sign network communications and verify the authenticity of parties to a transaction, which helps to prevent communications between machines from being hijacked or otherwise interrupted. Certain older operating systems aren't capable of meeting these security requirements, at least by default, and as a result are unable to interact with Windows Server 2003 domain controllers. Such operating systems are Windows for Workgroups, Windows 95 machines without the Directory Services client pack, and Windows NT 4 machines prior to SP 4. You'll also find that Windows Server 2003 DCs by default require all clients to digitally sign their server message block (SMB) communications.

The SMB protocol allows Windows systems to share files and printers, and enables various remote administration functions, as well as logon authentication over a network. If your clients are running one of the operating systems mentioned previously, and upgrading them to a later revision isn't an option, you'll need to turn off the digital signing and SMB signing requirements. Do this by disabling the 'Digitally sign communications' policy in the Default Domain Controller group policy object that applies to the OU where the domain controllers are.

Additionally, Windows Server 2003 domain controllers require that all secure channel communications be either signed or encrypted. Secure channels are encrypted 'tunnels' of communication through which Windows-based machines interact with other domain members and controllers, as well as among domain controllers that have a trust relationship. Windows NT 4 machines prior to SP 4 aren't capable of signing or encrypting secure channel communications. If NT 4 machines at a revision earlier than SP 4 must participate in a domain, or a domain must trust other domains that contain pre-SP 4 DC machines, then the secure channel signing requirement needs to be removed. This is also in the domain controllers' security policy, under the group policy object entitled 'Digitally encrypt or sign secure channel data'.

WRAPPING IT UP

The process for planning, strategising and performing any environment upgrade of this magnitude is always unnerving. But, using the strategies found in this feature and a bit of common sense, you can relax, knowing that you likely won't need backups restored or disaster recovery plans activated.

Jonathan Hassell is an author and consultant specialising in Windows administration and security. He is the author of *Managing Windows Server 2003* and *RADIUS*, both published by O'Reilly & Associates, and *Hardening Windows*, published by Apress.