Managing NT Domains

Once your user base exceeds 40,000, your system will be unable to exist in one domain and you'll face a choice of how to structure your domains. Until the forthcoming release of Microsoft's ADS the only viable alternative to NT domains is to use NDS for NT, which actually works rather well.

By Simon Pride

The word "domain" in Windows NT is used in a particular and specialised way. The term is more familiar than it used to be, as it is often used these days to refer to a particular location on the Internet. For instance, a commercial organisation called BigCorp might register and own the Internet domain bigcorp.com.

The use of "domain" in Windows NT administration in versions 4.0 and below has almost nothing to do with the meaning above, although in Windows 2000 (formerly Windows NT5) the two meanings are very closely related.

In NT4 and below it is instead used to refer to a collection of networked computers that share a common security database and security model. Security defines a domain; it has no other important attributes. For example, the range of TCP / IP addresses of computers in an NT domain is irrelevant, whereas in an Internet domain they are highly relevant.

In practice, when a user logs on to a networked NT computer they will usually be doing so in an NT domain. When the user presses the Secure Attention Sequence (Control-Alt-Delete) and enters their credentials, the dialog where they enter their user identifier and password will contain a third field, Logon From. This field will normally contain the name of the NT domain which the workstation belongs to.

When the user enters a user identifier and password, the information is sent (encrypted) over the network to a computer running Windows NT Server which is working as a Domain Controller. The Domain Controller validates the user credentials against its security database and, should the credentials be valid, allows the user to log on and use the computer and any authorised network resources in the domain.

A domain is therefore nothing more than a set of networked computers which look to one or more Domain Controllers to grant access to shared resources.

Within the domain, the security database (often called the SAM, for Security Accounts Manager, named after the Windows NT process which administers security) keeps track of which users and groups are permitted to do what with which resources in the domain. Every time a user wishes to use a resource, the user's permissions and rights (actually the contents of the user's Access Token, created at the time they last logged on) are compared with the resource's Access Control List as defined in the SAM on each Domain Controller. If the user has the correct permissions the operation proceeds; if not, it is refused.

Within the domain there is a separation of roles between the servers which maintain the domain, which might not be obvious to readers familiar with similar shared-security environments such as Novell's NDS (NetWare Directory Services) or Sun's NIS+.

In a Windows NT domain, one single computer in the domain is designated the Primary Domain Controller (PDC), and is the ultimate authority for all security information in the domain. It is assisted by Backup Domain Controllers (BDC), which may or may not exist in the domain. The crucial distinction between a PDC and a BDC is that changes to the domain's security model can only be made on a PDC. This fact underlies much of the accepted practice in designing NT networks and will be referred to later in the section on domain planning.

The role of a BDC is to cache the security model disseminated by the PDC and to validate logons and resource usage requests when the BDC is logically "nearer" to the requestor than the PDC. Needless to say, PDCs replicate the current security model to BDCs on a regular basis, but unlike NetWare's NDS there is no bilateral replication as there is between servers holding replicas of the NDS tree. A BDC in NT is similar to a read-only replica of an NDS partition.

"At several points in the lifetime of an enterprise you may need to rename a domain, perhaps to fit in with a departmental name change arising from a split, merger or change of focus."

Domain Structures

The simplest domain model is of course a network with one PDC and zero or more BDCs, on one single TCP / IP subnet, at a single geographical location. Every workstation on the network can reach either the PDC or a BDC with a sufficiently recent copy of the SAM information to reflect the permissions needed by workers at that point in the organisation's evolution.

A single administrator can grant permissions to use shared printers, read from new shared folders on servers and so on. This is an extremely efficient setup, and provides few problems for either the administrator or the users.

Unfortunately for administrators, when an organisation is efficient and effective it begins to grow. Growth can be organic - the organisation takes on more staff - or by acquisition of weaker rivals in the same business area. Either way, the administrator eventually has to confront the problem that a part of the enterprise is geographically remote from the first network that encompassed the original company. At this point some concerns militate against the single domain model.

Firstly, geographically remote offices, even if they are in the same city area, have to be linked with Wide Area Network (WAN) connections which, while swift, have performance issues and (much more importantly) cost implications when compared with the ordinary Ethernet LAN.

The cost implications arise when a change needs to be made to the existing security model; that change can be as humdrum as adding a new user account or even changing a user account's password. In every case, the change can only be made on the domain's PDC. If this change is attempted from an Administrator's workstation in a satellite office, the copy of User Manager for domains on that computer will contact the PDC in the main office via the corporate WAN in order to process the transaction.

This is undesirable from two perspectives: the delay and possible failure of the operation due to slow network links, and the cost implications where WAN connectivity or bandwidth is provided on an as-needed basis, which is typified at present by ISDN connections.

Secondly, the satellite or branch office might have its own management structure, often extending down into the administration of IT resources. In the case of a company that has been acquired it is often expedient to retain their IT staff to provide local, responsive and knowledgeable support to their users. These support staff will need some degree of administrative authority over their users which cannot be provided from a centralised resource, either because of staffing issues or because of the cost implications discussed above.

Finally, Windows NT Server has a limit of around 40,000 users per domain (the SAM database has a hard limit of 40 MB). If your organisation grows beyond this number of users you will be forced to create additional domains. Even if you don't reach those numbers of staff you may be constrained by SAM size; the SAM must fit completely in server RAM. As the SAM size is roughly (number of user accounts x 1 KB) + (number of machine accounts x 0.5 KB), a single domain with 100,000 employees all using NT Workstation will create a SAM of 146 MB. Even today, very few servers have so much memory that they can afford to allocate nearly 150 MB just to the SAM. On the average server the RAM allocated to caching the SAM will start to have a significant effect on server performance long before the physical RAM is exhausted.

It is therefore clear that a real-world network infrastructure using Windows NT will inevitably involve multiple domains sooner or later, and a strategy for managing these domains should be on every administrator's agenda. In the next section I review the common models of arranging multiple domains, but first I need to discuss the mechanism whereby domains can interact - the Trust Relationship.

Trust Relationships

I said above that a domain is a set of Windows NT computers that share a common security database and model. The upshot of this is that users from one domain cannot even use the workstations in another domain to log into their own home domain without special arrangements undertaken by the domain administrators. Those arrangements are called Trust Relationships, or more commonly abbreviated as "trusts".

A basic trust relationship is one-way. Domain A will agree to trust accounts validated by domain B, but that doesn't mean that domain B will automatically trust any account validated by domain A. In order to do that, another trust in the opposite direction must be established by the administrators of the two domains.

What does a trust relationship actually mean? At first glance it might seem to mean very little - all a trust does is permit accounts from domain B to be added to the list of accounts in domain A which may use a resource in domain A. Domain B's accounts can't automatically use domain A resources just because the trust has been established; like every other NT account they must be granted permissions to resources in domain A.

The one exception to this rule is where a resource in domain A has permissions defined for the group Everyone. After a trust is established, the meaning of the group Everyone in domain A changes to "all user accounts

"Within the domain, the security database keeps track of which users and groups are permitted to do what with which resources in the domain."

NT Domains

"One of the best ways to manage an enterprise network is to sidestep the domain issue completely and use a directory service instead."

and guests from both domain A and domain B". In this case the domain B users will "leak" into domain A's resources without further action. It is part of best practice to remove Everyone from visible network resources and replace it with permissions tied to defined groups that have valid business needs to use those resources.

Creating a trust is easy but not wholly straightforward. The process involves two steps: first the trusted domain must permit the trusting domain to trust it, and then the trusting domain is set to trust the trusted domain. In this example domain A will be set to trust domain B.

1 Log onto the trusted domain (domain B) as an Administrator and run User Manager for domains.

2 Select Policies / Trust Relationships. The Trust Relationships dialog will open.

3 On a new network the Trusted Domains and Trusting Domains list boxes will be empty. Click the Add button next to the Trusting Domains list box.

4 The Add Trusting Domain dialog appears. Type the name of the domain you want to allow to trust your domain in the top field. In our case the trusting domain is domain A.

5 You will be asked to supply a password and confirm it by retyping it. This does not need to be an Administrator password or even an existing password in the domain - any password will do, as will leaving the password fields blank. The password is only used during the process of trust creation, and does not form part of the domains' security models (you don't even need the password to delete the trust, which seems a little sloppy).

6 Click OK and then close the dialog.

Now go to domain A and again log in as that domain's Administrator. Go to the same dialog in User Manager for domains.

1 This time click Add next to the Trusted Domains list box. The Add Trusted Domain dialog appears.

2 In the domain field type the name of the trusted domain (domain B).

3 In the Password field type the password you used in step 5 above.

4 Click OK.

5 Domain B should now appear in the Trusted Domains list box.

6 Exit the dialog.

Even though a trust has been established, domain B users cannot start to use domain A resources until they have been given permissions to do so. This process is similar to granting permissions in a single domain, but with one extra step.

Imagine you wish to give permissions to use \\SERVER1\SHARE1 to a group from domain A.

1 Either right-click the folder you wish to modify and choose Sharing / Security / Permissions, or run Server Manager, select \\SERVER1 and choose Computer / Shared Directories. Select \SHARE1 and click Properties / Permissions.

2 Click Add... to display the Add Users And Groups dialog. At the top of the dialog look at the combo box labelled List Names From. This will show the current domain (domain A). Click the drop-down arrow, and you should see the name of the trusted domain (domain B) as well as the current domain. Select the trusted domain (this is the extra step).

3 The Names list box will now show the groups from domain B. If you need to add individual users (remember all user permission management should be done via groups, even for a single user), click the Show Users. [*See "How To Manage NT User Accounts", PCNA 108, File T1711 - Ed.*]

4 Select the accounts from domain B which are to be permitted to use the share, set the level of permission from the Type of Access combo and click Add, then click OK.

5 You will return to the Access Through Share Permissions dialog. The list box should now show all users of the share from both domains, with those from the trusted domain having a prefix of their "home" domain name before the account name. Click OK again, and once more to exit the Share Properties dialog.

"In a Windows NT domain, one single computer in the domain is designated the Primary Domain Controller."

The users from the trusted domain (domain B) can now use SHARE1 on SERVER1 of the trusting domain (domain A).

The procedure above assumes something about how your network is arranged and staffed: either that one administrator can easily visit both domains, or that there is a competent administrator at both sites. However, it is often the case that one administrator has to look after several geographically-dispersed domains. Using the procedure above would mean trusting an inexperienced user with an Administrator account or physically visiting the site of each domain.

There is a technique whereby both ends of the trust can be established from one side of the relationship - providing you have the Administrator account password for both domains.

To make a remote domain trust the domain you are currently at, first permit the remote domain to trust your domain as outlined above. Normally you would now have to go to the other domain to complete the process. However, the following can be done from the trusted domain:

1 Choose Start/Command Prompt and issue the command

NET USE \\trustingdomainPDC-\IPC$ /USER:trustingdomain\-Administrator

where trustingdomainPDC is the NetBIOS name of the PDC of the trusting domain and trustingdomain is the domain name of the domain you want to allow to trust the current domain.

2 When prompted for a password, enter that of the trusting domain's Administrator account.

3 Return to User Manager For Domains, and choose User/Select Domain. You will not see the trusting domain in the list, but you can still type its name in the edit box. The current domain will change to the trusting domain.

4 Now choose Policies/Trust Relationships and complete the trust setup as if you were sitting in the trusting domain.

Complete Trust

Having surveyed the meaning and creation of trust relationships, let's go back to looking at domain models. Assuming you choose to, or are forced into creating more domains for your network, then the complete trust model is the next most simple arrangement.

In the Complete Trust model, every domain trusts every other domain. This means that any user can use any resources in any domain where they have permissions. For a small number of domains this is a simple way of extending the model of the single domain without too much effort. However, this is not a model that scales well.

Remember that trusts are only between pairs of domains; every time you create a new domain you must establish trusts between it and all other domains. The number of trusts to be created increases semi-geometrically with the number of domains, so for two domains two trusts are needed; for three domains six are needed, for four, 12 and so on. By the time you reach 10 domains the effort of keeping track of the trusts becomes a significant burden in itself. The formula for the number of trusts needed to maintain complete trusts across N domains is N^2 - N, which for 10 domains gives 90 trusts.

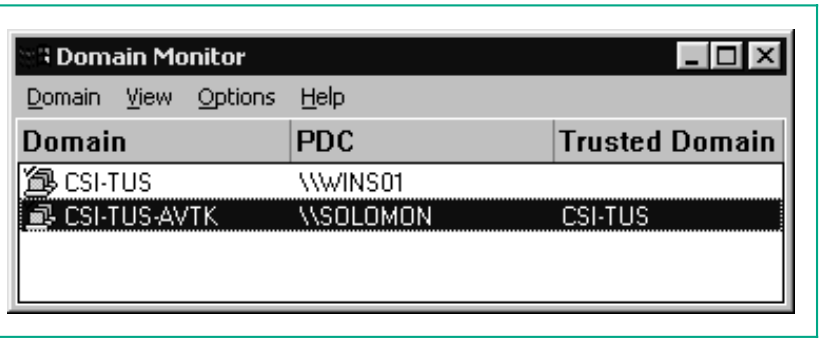

Figure 1 - The Domain Monitor utility.

Master/Resource Model

As a compromise between a single domain and complete trust, Microsoft suggests the master/resource domain model. One domain, the master domain, contains all user accounts for the enterprise but only the machine accounts for its own servers. All other domains - the resource domains - contain resources the users might want to access, such as servers, shares and printers, and the machine accounts for the servers and workstations in the domains.

Resource domains are set to trust the master domain, but no resource domain trusts another, nor does the master domain trust any resource domain. To illustrate how this works in practice I need to digress again and explain the difference between local and global account groups in NT.

When you create a group on an NT server, you have to specify whether it is a global or local group. A local group can contain user accounts or other groups, providing they are global groups. A global group may contain accounts but no other groups. At first glance it might seem that the designers of NT have got this nomenclature the wrong way round - "global" sounds bigger than "local", but a local group can contain a global group. However, the names are based on the following reasoning: global groups can be used anywhere on the network, but the use of local groups is confined to the domain where they were defined.

We can therefore now see how the master/resource domain model fits together: all user accounts are held in global groups on the master domain, and local accounts are created in the resource domains which grant access to the specific resources, and then the relevant global groups are added to

NT Domains

the local groups in the resource domains.

You should also place the users or groups from the master domain who you want to be able to administer the servers in the resource domain into the Administrators group in the resource domain. Usually the master domain's domain Admins group is used for this purpose.

The great advantage of the master / resource domain model is the centralised administration of user accounts, but the devolved administration of resources. However, there are disadvantages as well. If the master domain is not available, nobody in the enterprise will be able to log on. Furthermore, as the number of accounts increases so will the strain on the PDCs as described above. Finally, you may reach the hard limit on the SAM database size much earlier, since all accounts are in the one domain.

Multiple Master Domain

A partial solution to the issues above is to have more than one master domain (partial as it does not address the very real availability issue). User accounts can be divided up between two or more master domains that are each trusted by the resource domains and trust each other. However, that brings one huge drawback over the single master domain model.

Recall that global groups can't contain other global groups, so you can't create a global group containing every user in the enterprise by simply adding one domain's group into the other's. Nor can you use a local group on one master domain containing global groups from it and the other master domains, because local groups cannot be used in the resource domains. You must therefore add two or more global groups to each resource domain's local groups every time you create a new local group.

Renaming A Domain

At several points in the lifetime of an enterprise you may need to rename a domain, perhaps to fit in with a departmental name change arising from a split, merger or change of focus, or latterly to prepare for migration to Windows 2000 (formerly Windows NT 5.0) where domain names and DNS names are closely aligned.

"By the time you reach 10 domains the effort of keeping track of the trusts becomes a significant burden in itself."

Check services using domain accounts (not System or local accounts). Stop them and set their startup to Manual to prevent them trying to start up after a reboot.

Trusts use the domain names as part of the information about the trust and will not "convert" automatically when a participating domain's name is changed. You will need to document all your existing trusts before beginning the renaming process. If you have the Server Resource Kit you can use the Domain Monitor utility to show for each domain its PDC and the domains it trusts (see Figure 1). Once you have documented them you must break all existing trusts.

The last step before the actual process is to halt all network activity for the duration. Log off every workstation that connects to the domain, and pause or stop the Server service on all servers.

Now go to the PDC and choose Start / Settings / Control Panel / Network / Identification and click Change. Enter the new domain name and click OK. You will receive a warning that connections with domain members will be lost and that you will need to change the domain name on all servers and workstations. It also offers a last chance to abort this process should you wish. If you are ready, click Yes. You will be told to reboot the machine, which you should do immediately.

The PDC has now established the new domain. However, any services which use domain accounts will still have the old domain name and will not be able to log on. Start the Control Panel / Services applet and, for each such service, choose Startup and examine Log On As / This Account. You must change the domain element of the account name to the new domain name, either by editing the domain name directly or choosing a new domain account from the account browser dialog box.

Because of a bug in NT, this must be done in two steps. First set the service to use the System account and press OK. Now click Startup again and change the account to use the new domain account. If you try to do this in one operation it will fail - NT will complain that the new account doesn't exist (error 1057).

You can now move onto the BDCs, and carry out the same operations there. One point to note is that if a BDC has any sort of connection to the PDC it won't let you change the domain name - you will get the error "You already have a connection to the domain...". If this happens check that there are no open connections between the BDC and PDC (use Server Manager on the PDC, and look at Users, Shares and In Use. Clear down any connections and try again). In extreme cases with poorly-written services you may need to reboot the machine.

Once you have changed the name, go over to the server and fix up services using domain accounts as above. Member servers and workstations are treated the same way as BDCs. Don't forget to create new Emergency Recovery Disks (ERDs) for all machines, as the domain name is encoded on the disk. Repairing a domain controller with an out-of-date ERD will restore the old domain name and have disastrous effects on your network.

Once you have reconfigured all the computers in the domain you should go to Server Manager and synchronise the entire domain.

There is an alternative to visiting every workstation in order to rename the domain they should join, provided

you have the NT Server Resource Kit. The Resource Kit utility NETDOM.EXE can be used to remotely change the workstation's domain membership. To move a workstation to a new domain name issue the command

NETDOM /DOMAIN:<renamed domain> MEMBER <workstation> /JOINDOMAIN

See the documentation for NETDOM for further examples.

Remember that on Windows NT you can use a text file containing the NetBIOS names of your workstations and member servers together with the FOR command with the /F switch to apply the command to each computer listed in the file. If WORKSTATIONS.TXT contains a simple list of computers, one name per line, then the command

FOR /F "tokens=1" %a in (WORKSTATIONS.TXT) DO NETDOM /DOMAIN:<renamed domain> MEMBER %a /JOINDOMAIN

will join each computer to the new domain.

Third-Party Tools

Tools exist to help with the process of domain configuration. One product, DM/Manager, from FastLane technologies (www.fastlanetech.com) can simplify the overhead involved in moving users between domains. It can automate the migration of user accounts and global groups between domains, which otherwise would have to be laboriously recreated in a new domain.

NDS For NT

One of the best ways to manage an enterprise network is to sidestep the domain issue completely and use a directory service instead. Microsoft is promising enterprise-wide directory services in Windows 2000 in the shape of Active Directory Services (ADS). However, Novell's (www.novell.com) NDS for NT is a credible alternative and has been available since late 1997.

Whereas previous versions of NDS for NT concentrated on keeping NT and NetWare networks in synchronisation with each other, the latest iteration of the product actually replaces the NT domain and trust security model with the Novell Directory Services (NDS) tree.

The NDS tree is a hierarchically-structured database containing the various objects which comprise a computer network: servers, printers, groups (or Organisational Units in NDS terminology) and users. User permissions and rights to resources, and group memberships, are administered directly in the NDS. This is achieved by replacing the NT components which provide domain security (principally SAMSRV.DLL) with ones which redirect authentication requests to the NDS tree running on a NetWare 4.0 or higher server.

Novell is working on a version of NDS/NT that will be completely native on NT - ie, it will no longer require the presence of a NetWare server.

Since NDS is an enterprise directory with none of the NT system's size or networking constraints, there is no need for NT domains and trust relationships. Users in one Organisational Unit (OU) container can be given permissions to use local resources (held either in their local OU or particular resource containers) or ones in a completely functionally and geographically remote OU, without any special arrangement. It is not even necessary for workstations to run Novell's Client32 access software unless they need access to NetWare servers; however, any existing PDCs and BDCs must run the latest version of this client to communicate with the NDS tree.

The NDS software even has a Wizard which automates much of the work in migrating existing domain accounts into an NDS tree. An added bonus of the system is the Novell Workstation Manager (which does require the presence of Client32) which can implement user and workstation policies and profiles in the same way that a native NT system does, but with the advantage that all policy objects are stored in and administered from the NDS schema.

When a user logs into a network using NDS, the policy objects for user and workstation are applied to that session, and a temporary local account is created on the workstation, without which the user would not be able to log on.

The account is removed at the end of the session, which sometimes leads to an interesting situation when restrictive local file security is in force. Files are sometimes left on the local hard disk by the user, with the intention of returning to them at a later time. However, because the local account is created anew every time the user logs on, the SID of the new session's account will be different from that under which the files were created, and therefore the user will no longer own "their" files and will be unable to use them.

Such minor inconveniences aside, NDS for NT is a mature and scalable solution to the domain management jungle, which Microsoft's forthcoming ADS will have to work very hard to better.

PCNA

The Author

Simon Pride (simon.pride@itp-journals.com) works for the University of Cambridge Computing Service, advising on PC systems and networking.

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.