The Win2000 Active Directory

In Windows 2000 almost everything revolves around Active Directory. Many new features are included to make networks simpler to manage and easier to secure, and add-on client software is even available for computers running Windows 95 and Windows 98.

By Dave Cook

Imagine for a moment a vast network of operating systems that requires neither constant attention nor frequent adjustment to keep it running. The network would be flexible, stable, scalable and secure. It would be compatible with all hardware devices and software applications, and it would be able to run any application on just about every type of computing device, from the smallest notebook to the largest mainframe.

An impossible dream? Perhaps. Windows NT is certainly not up to the task. Its scalability, for instance, is poor, with a flat-file registry-based security system that has caused - and will no doubt continue to cause - more than its fair share of problems. What NT lacks is a true directory service - one that is capable of handling the management tasks of a huge, almost infinite network of users.

In Windows 2000 Server Microsoft has achieved that goal - and more - with Active Directory. Although Active Directory can be installed the first time Windows 2000 Server signs on, its immediate implementation is not compulsory. Indeed, because many administrators may need to familiarise themselves with Windows 2000 and its concepts, there are good reasons not to install Active Directory at this time.

Administrators who decide to install Active Directory later can do so from the Configure Your Server wizard (Figure 1), which is available from the Start | Administrative Tools menu.

Directory Service

At its most basic level, a directory service can be regarded as a type of telephone directory for businesses. Entries in this directory would fall under certain categories such as Plumbers, Hairdressers, Caterers, and Car Hire, and each entry could contain certain attributes, such as Name, Address and Phone Number. In order to provide further details about the business, additional elements are often included. For example, this could be information regarding a company's products, slogans, maps, and any specialist areas in which it may excel.

A network directory service is rather more complex than the average telephone directory, of course. Nevertheless, the concept remains the same: Active Directory contains entries for users and groups, workstations and servers, printers and queues, and so on and so forth. It can store, organise and retrieve information regarding all ob-

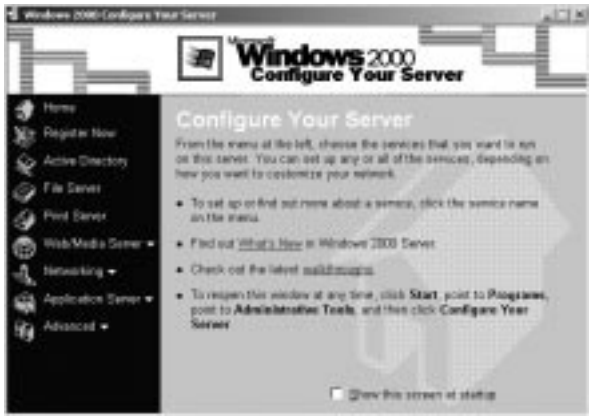

Figure 1 - Active Directory can be installed at any time using the Configure Your Server wizard.

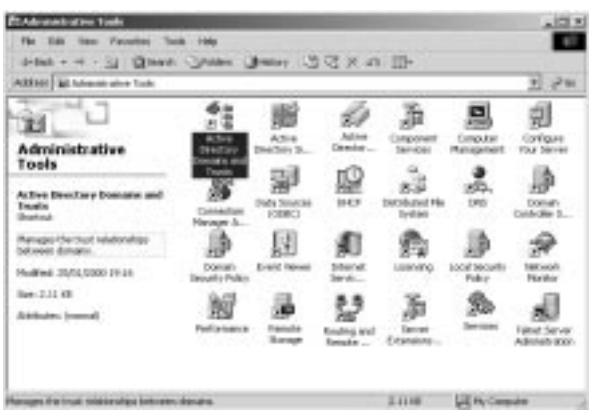

Figure 2 - The most influential Active Directory snap-ins are available from the Administrative Tools menu.

jects of interest that may be held on any of its networks.

Many enterprises already have different directories in place. For instance, network operating systems, electronic mail systems and groupware products could all have their own directories. However, various issues can arise when a single enterprise deploys multiple directories - issues often associated with usability, data consistency, development and support costs, among others. Active Directory, on the other hand, addresses these issues by aiming to provide a consistent and open set of interfaces for managing and using multiple directories.

Unfortunately, while there are still backup Windows NT domain controllers in the network, Windows 2000 must be run in what is known as mixed mode. Since mixed mode allows for neither universal nor nested groups, it is generally a good idea to upgrade any existing NT domain controllers shortly after. Only then will Windows 2000 be able to run in its more comprehensive native mode.

Schema

Such is the scope of Active Directory that it can oversee every object in a system, allowing those objects to be managed centrally and more easily. Objects that can be stored in Active Directory are identified as the schema.

Active Directory includes a default schema, which defines various object classes such as users, groups, computers, organisational units (OUs) and security policies. Because Active Directory is also extensible, it is possible to add new classes of objects to the schema, as well as adding new attributes to existing classes of objects. This can be accomplished programmatically, through Active Directory Services Interface (ADSI), or by using the Schema Managing snap-in tool.

Be aware, though, that Active Directory does not support the deletion of schema objects. Instead, schema objects can be marked as deactivated. Extending the schema itself is quite an advanced operation with the potential for adverse consequences. As such, Microsoft recommends the schema to be extended programmatically. It is also worth noting that each new object and property that is added to the schema requires a unique object identifier (OID).

Trees And Forests

Unlike the flat, downlevel directory services in Windows NT, Active Directory is hierarchical. Domains are all-important and are used as boundaries for security, administration and replication. A company's resources are stored logically to form closely-related trees with contiguous namespaces, or into loosely-linked forests of domains that trust each other.

This makes resources in even the largest of networks easy to find and manage. Typically, users can search Active Directory for a unique printer located nearby, find files on a network, or look for a group of users managed by a particular individual.

The three primary tools administrators will use when working with the directory can be accessed from the Active Directory Microsoft Management Console (MMC) snap-ins: AD Domains and Trusts, AD Sites and Services, and AD Users and Computers. These tools are accessible by clicking on Start | Programs | Administrative Tools (Figure 2).

Domains

In Windows NT networks, the structure of a domain is reflected in the relationship between master user domains and resource domains. To form these relationships, an administrator would typically choose from one of several domain models. For example, a single domain, a single master domain, a multiple master domain, or a complete trust model.

Often the administrator is left with little option but to choose a particular domain model in order to comply with certain constraints unique to Windows NT. Keeping within the limits of the Security Accounts Manager (SAM) is one example, while complying with the delegation of certain administrative tasks is another. Due to the technical limitations of Windows NT, many organisations are more or less pushed into implementing multiple domains. When designing a Windows 2000 domain, however, it is important to realise that these restrictions no longer exist.

Domains built with Active Directory can store millions of objects, offering administrators far greater control over domain size and structure. Moreover, because Active Directory is extremely flexible, the type of objects and properties stored can be unique to your users' own requirements.

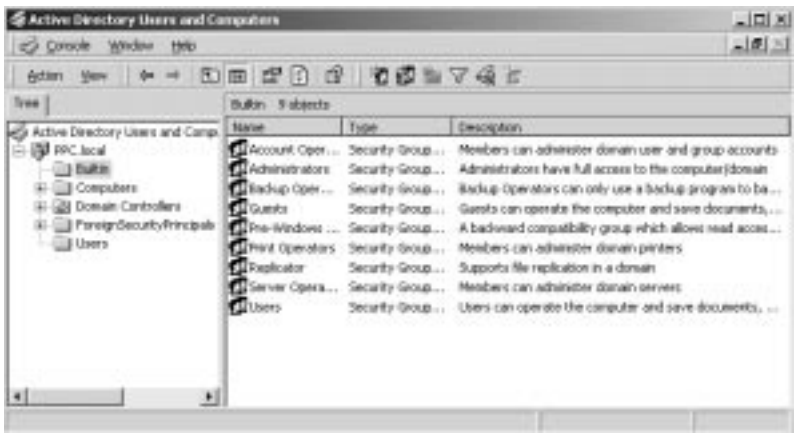

Figure 3 - A ready-made set of default groups is provided in the Builtin and Users folders, which are part of the Active Directory Users and Computers Console.

Active Directory

Each domain can create its own domain policy objects, or it can store replicas and links to domain policy objects elsewhere in the tree. When replicating from another domain, a global catalogue server automatically handles replication, with the domain object storing the link to a domain policy object.

In downlevel networks, domains are the smallest units that can be used to group resources. But this is not so with Windows 2000, which uses organisational units to organise container objects within the domain. In other words, OUs allow administrators to assemble objects such as users, groups, computers and other information into a usable hierarchy.

Since the structure of a Windows 2000 domain is radically different from a domain created with Windows NT, using an NT domain model as the basis for a Windows 2000 design is not recommended. Instead, Windows 2000 domains should be based on the company's physical, operational and administrative characteristics.

Administrators also need to be aware that a DNS domain is required to host each Active Directory domain, and that, when Active Directory is implemented, administrators will effectively be introducing an intranet to the organisation. This is a prospect that some NT administrators might find unnerving - especially since many of them will have had little or no experience of DNS, let alone of running an intranet.

Partitions

Unlike in Windows NT, there is no master-slave replication relationship in Windows 2000; rather, every domain controller is a master. Moreover, every Windows 2000 domain is actually stored as a partition in the Active Directory, and each partition holds the values for every interesting object along with each of its properties.

Domain controllers in other partitions can replicate this partition to share things, with each controller having the capability to have Read / Write copy of the partition. Active Directory replicas can also be used to provide fault tolerance and to improve performance across the network.

In many cases, small and many medium-sized companies will require only one domain. However, larger companies may need several domains - due, in part, to the traffic generated by replication updates between domain replicas. This is when the benefits of Active Directory are most apparent.

Trusts

The multiple domains of Windows 2000 are linked through trust relationships using the Kerberos protocol. Kerberos trusts can be both transitive and hierarchical. They can be applied throughout a domain tree and may be extended by linking top-level domains together.

In Windows 2000 all trust relationships are created automatically, allowing users to share resources with every domain in a network. Some trust relationships can be quite complex. However, an example of a simple transitive trust is: if domain A trusts domain B, and domain B trusts domain C - then domain A would also trust C.

One-way non-transitive trusts may also be created, of course, although transitive trusts usually make the administrator's task far easier. Transitive trusts simplify resource sharing enormously, eliminating much of the hassle of configuring and managing one-way relationships.

Permissions

Transitive trusts allow users to share resources, but to access resources users require permissions. Active Directory allows administrators to grant permissions for objects to single users as well as to local, global and universal groups. It achieves this because every object in Active Directory has an Access Control List (ACL) that contains Access Control Entries (ACE). These entries define which users or groups have permissions for each object.

Credentials and access permission information are stored so that, when users log on, they are given access to system resources on the basis of permissions. In order to keep projects manageable and to simplify network maintenance, it is recommended that permissions should be granted to groups rather than to individual users.

The advantages of this are fairly straightforward. For example, once a list of permissions has been assigned to a particular group, individual users - as appropriate members of the group - can be assigned to automatically receive all the rights and permissions previously assigned to that group. For the members to automatically inherit any future changes, the group's privileges only have to be changed once.

Windows 2000 actually provides a set of default groups, which can be found in the Builtin and Users folders

Remote Access

In order to access databases remotely, Active Directory brings into play two well-known Internet standards: Lightweight Directory Access Protocol (LDAP) and the Domain Name Service (DNS).

- Based on the X.500 foundation, LDAP is used for querying, accessing and managing objects stored in directory services. Because LDAP is a standard directory-access protocol that defines how to access information held in a directory, it means that off-the-shelf applications using LDAP may also access Active Directory to find objects stored there.
- The introduction of a native and dynamic DNS, frequently referred to as DDNS, leads to the end of the unpopular Windows Internet Naming Service (WINS) that converted Microsoft NetBIOS names to DNS names. Since Windows 2000 domain names are based on DNS names, DDNS can be used for locating machines (including Active Directory Domain Controllers) and services using standardised names. To do this, administrators would use the command-line utility, NSLOOKUP.

of the Active Directory Users and Computers Console. In fact, these are security groups, representing pre-ordained configurations that allow administrators to assign roles, rights and permissions to all manner of users and groups.

Be aware that the Builtin groups folder (Figure 3) contains the default groups relevant only to that particular domain. The Users folder, meanwhile, contains pre-defined groups with limited scope. Although Builtin groups can be moved to other groups or OUs within a specified domain, they cannot be moved into other domains.

"Active Directory contains entries for users and groups, workstations and servers, printers and queues, and it can store, organise and retrieve information regarding all objects."

Client

For client access to Windows 2000 Active Directory networks, AD client support is built-in and provided with all versions of Windows 2000. Add-on AD client software can be installed on computers running Windows 95 and Windows 98, but not, at the time of writing, on Windows NT machines.

In order to achieve AD client support, administrators are thus left with two options: install the add-on AD client support for Windows 9x, or upgrade to Windows 2000 Professional. It is important to note, however, that installing the former will not make the user a fully-functioning member of the Active Directory domain.

Nevertheless, add-on client support will be of benefit to those organisations that have decided to wait until the first couple of service packs have been released before upgrading to Windows 2000. Add-on client support can be found on any of the Windows 2000 Server installation CDs in the ClientsWin9x folder. Simply double-click on the DSCLIENT.EXE file to begin the setup program. It is a fairly straightforward process and wizard-driven. For the Active Directory client to install properly, however, Internet Explorer 4.0 or higher must be installed on the Windows 9x computer.

While add-on client support for Windows 9x is far better than nothing, it is not as advantageous as upgrading client machines to Windows 2000 Professional. It does, however, have one benefit. Unlike the full upgrade, the directory service client can easily be uninstalled from the Add/Remove Programs applet, accessed from the Windows 9x Control Panel.

Conclusion

Microsoft's Active Directory certainly has a lot going for it, though it must be stressed that the planning stage is all-important. If your Active Directory design is good, your users and ultimately your organisation will reap the rewards. Above all, it is its scalability - the capability to accommodate a wide range of network sizes and complexities - that should make it a winner for the typically expanding organisation.

If there is a downside to using Active Directory, it is that it should not be initiated lightly. Before implementation, spending some time learning about Windows 2000 and its new features is not only recommended, it is essential.

Goodbye SAM

Windows NT 4.0 stores objects using the Security Accounts Manager (SAM) database. Its maximum size is recommended to be 40 MB or less. Although much depends on how groups and computer accounts are used, this recommended limit could allow the grouping of approximately 40,000 users in a single domain.

Active Directory domains, however, can be up to a massive 17 TB (terabytes) in size. Needless to say, a domain that size can support millions of objects. The type of objects and properties stored can be unique to the requirements of each organisation.

Further Information

www.microsoft.com/hcl/
Microsoft hardware compatibility list
www.microsoft.com/hwdev/
Development and testing site
www.microsoft.com/windows2000/compatible/
Latest application compatibility information
www.osr.com
Driver development site
www.alvestrand.no/objectid/
More on OID registrations

PCNA

The Author

Dave Cook is a freelance journalist and technical consultant. You can contact him by email at dave.cook@itp-journals.com.

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.