

# Designing Your Windows 2000 Active Directory

By Linda Chapman

**The design and deployment of Windows 2000 Active Directory has several considerations. The Active Directory design phase should include the forest, tree, domain, trusts, organizational units, Domain Name System, site boundary definitions, global catalog, and schema architecture. This article provides critical information that should be considered prior to the design of the Active Directory and deployment of Windows 2000.**

The directory service integrated into the Microsoft Windows 2000 Server and Windows 2000 Advanced Server operating systems offers many advantages over Windows NT Server 4.0. Directory Services provides access to information about people *and* resources on the network within one view and enables the user to search through the global catalog. Types of information found in a directory can include the following: names, locations, e-mail addresses, logins, passwords, computers, databases, printers, routers, servers, Distributed File System (DFS) volumes, and Group Policy Objects (GPOs).

## The Active Directory

Everything is simply an object in the Active Directory. Information about these objects is stored in the directory information base (DIB). Entries in the DIB describe and provide links to users and physical objects. The Active Directory uses the Domain Name System (DNS) as its locator service, organizes objects within domains into a hierarchy of organizational units (OUs), and allows multiple domains to be connected into a tree structure. The namespace can contain millions of objects, a significant improvement over the Windows NT Server 4.0 size and replication limitations.

The Active Directory provides a single point for administering all published resources in the network; it even provides access to application programs. Figure 1 shows the Active Directory structure.

Active Directory Service Interface (ADSI) abstracts the capabilities of directory services from different network providers to present a single set of directory service interfaces for managing network resources. ADSI is a set of extensible, easy programming interfaces that can be used to write applications to access and manage the Active Directory and any Lightweight Directory Access Protocol (LDAP)-based directory, including NetWare® Directory Services (NDS).

The object set and its available attributes are called the *schema*. The schema, which is stored in the Active Directory, makes object classes different from each other. The Active Directory provides the ability to extend the directory schema and to create new properties, objects, and custom data structures in the directory for applications, using the directory as a data store. One type of object is a container, which can be used to organize other objects and can be nested within other containers.

Domains represent a logical partition within the Active Directory for both security and directory replication. Domains relate directly to the DNS namespace and are, in fact, addressable through DNS. All network objects exist within a domain, and each domain contains a full set of its objects within the Domain Naming Context.

In the Active Directory architecture, trees are hierarchical structures of linked domains that form a contiguous namespace and share a common schema, configuration, and global catalog.

## Designing Your Active Directory

Several key elements are important to consider when designing the Active Directory:

- **Business model.** Consider your organization's key business objectives while designing the Active Directory namespace.
- **Administrative model.** Consider the importance of administrative responsibility at all levels of the domain hierarchy in your enterprise network.
- **Future growth and reorganization.** Design the Active Directory namespace to accommodate organizational changes.
- **Security.** Set policies and enable trusts that provide users with secure, authorized access to network data and resources.
- **The existing environment.** Determine a strategy for upgrading or migrating from the existing environment to the Windows 2000 environment. This includes planning for integrating distributed applications with Active Directory.

Once you have evaluated these business issues, you should consider some characteristics that are important to the Active Directory design:

- **Flexibility.** As the company changes, the proposed architecture must be flexible enough to be able to accommodate those changes without any visible change to the overall service provision.
- **Scalability.** As the company grows or changes its business model, the proposed architecture must be able to scale at a global level and have a design that can handle rapid growth by servicing hundreds of millions of objects.
- **Decentralization.** The proposed architecture should be designed so that no one entity can wield absolute control over the entire namespace.
- **Maintainability.** The proposed architecture should be user-friendly and modular so that various parts can be replaced or changed independently of others.
- **Globalization.** Directory design must accommodate the size of a growing organization, keeping in mind global expansion, or dispersion. Consider the global network

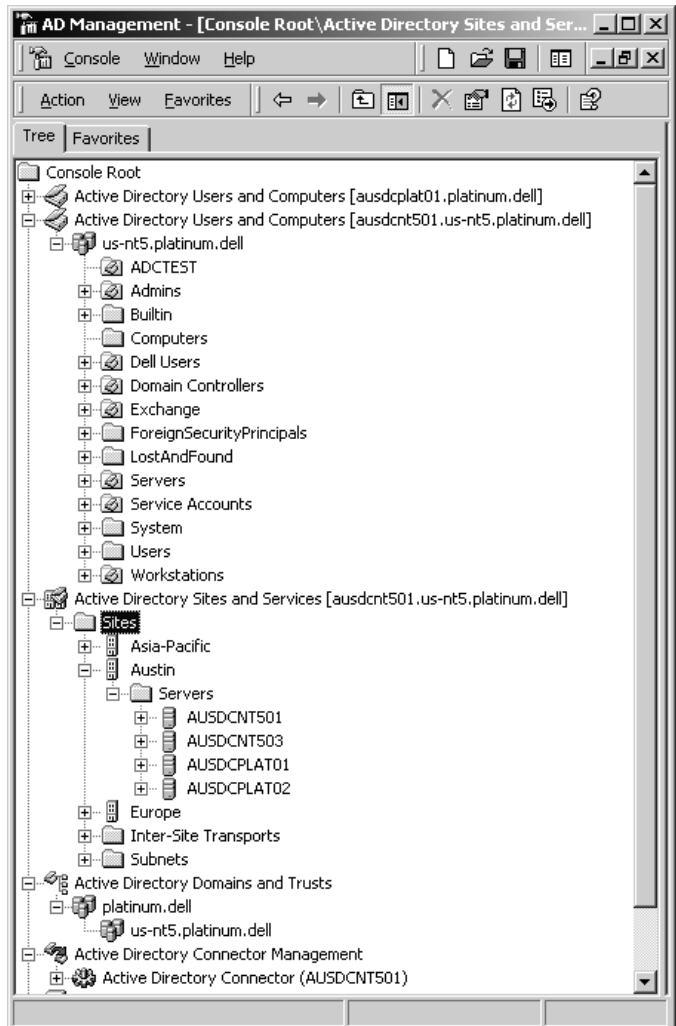


Figure 1. Active Directory Structure

topology and global administration and support needs. Identify whether there is a common set of services and/or management across regions and business units.

## Preparing the Windows NT Server 4.0 Environment

It is not necessary to wait. You can begin preparing your current Windows NT Server 4.0 environment for migration. The following tasks can be performed now to get your Windows NT Server 4.0 environment ready for migration:

- Perform a network discovery and document all computers; their purposes; operating system versions, including Service Packs; and application loads.
- Upgrade to Windows NT Server 4.0 any servers that are running previous versions, since Windows NT Server 4.0 provides the easiest upgrade path to Windows 2000.
- Consolidate all resources into as few domains as possible.
- Implement an enterprise-wide DNS structure. Choose one of the naming conventions supported by the Active Directory that best fits the needs of the organization.

- Simplify the Windows Internet Naming Service (WINS) architecture as much as possible. As you migrate to Windows 2000, you will still need to rely on WINS for NetBIOS resolution until you have eliminated NetBIOS altogether. In your plans for eliminating NetBIOS, be sure to check all applications for dependencies on NetBIOS.
- Become familiar with Windows Scripting Host to develop system administration tools and Microsoft Management Console (MMC) as a repository for those tools.
- Become familiar with Microsoft DFS, which provides the capability to create distributed file systems that spread across several servers. With DFS, the user does not need to know the names of the servers on which the information is stored.

Start testing now by establishing a proof-of-concept lab for product evaluation. Establishing this lab environment prior to deployment will help prevent engineers and users from “playing” with the new operating system on your production network. This will also provide an environment for application testing during your migration project.

Read the Microsoft Windows 2000 white papers and walk-throughs available on Microsoft’s Web site. Microsoft has done its best job yet in providing technical white papers and migration strategies prior to the product release. Take the time to read about subjects such as site boundaries, directory replication, global catalog servers, and indexing. Implementing new features like these without completely understanding their purpose and without fine-tuning can cause less than optimal network performance.

### Tree and Domain Architecture and Planning

There are many considerations in planning your Active Directory. Do not expect to get it right the first time. For

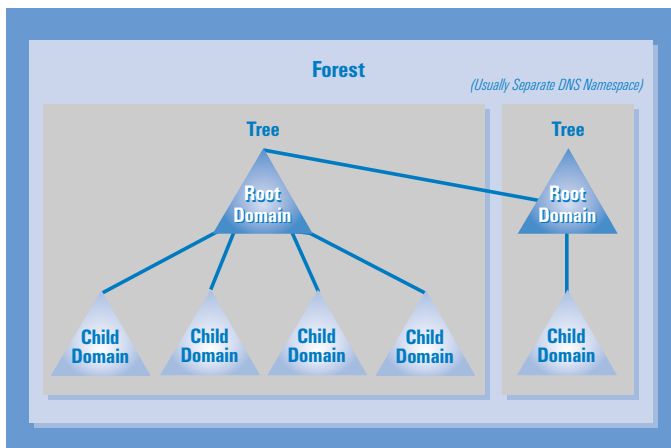


Figure 2. Forest, Tree, and Domain Structure

large environments, you may consider separating the planning into two or more phases.

First, design what you consider to be the ideal structure, even if it does not reflect your current domain or directory infrastructure. Although what is considered the ideal structure may not *seem* attainable in the current situation, it may be at a later date or under different circumstances.

Next, review your existing Windows NT Server 4.0 domain model and compare it to the business, support, and administration models and goals identified above. Then begin the design of your corporate forest, tree, domain, and organizational unit structure. Figure 2 shows the structure of a forest, with trees and domains.

Figure 3 shows the steps to follow when designing your Active Directory architecture.

Figure 4 shows an organizational unit tree structure. OUs exist for the delegation of administration and for the application of group policy and not to simply mirror a business organization. The default OUs are not represented in this figure: built-in, accounts, users, computers, domain controllers, and groups. Only a sample second tier is represented.

### Designing Security

Design the security model and policies for each level. With Windows 2000 and the Active Directory, you can become very granular with security. Allow yourself additional time for developing the security model, for there is much to learn.

### Managing Domains

Every Active Directory namespace design includes at least one domain. One domain is sufficient for most organizations, and it is easier to administer and maintain than multiple domains.

Several reasons can justify additional domains:

- The domain will contain more than 10 million objects.
- You can control replication if a reliable network connection is unavailable.
- Two or more groups in the organization have unique domain policy and security requirements. The domain boundary constitutes the security boundary.
- The organization responds to political requests for autonomous administration of departments or divisions.

### Collapse Resource Domains to a Hierarchy of OUs

In Windows NT Server 4.0, resource domains provide the means for delegating administration. Windows 2000 can reduce these administrative and hardware costs by collapsing the resource domains into a hierarchy of OUs. You can use the upgrade to the Active Directory to reduce the number of

domains in the environment, thus simplifying the network administration and network structure.

Additional OUs may be necessary to delegate administration, scope the application of policy, scope visibility of objects, or to replace Windows NT Server 4.0 resource domains.

## Preparing for Migration

The migration or deployment should be approached with the following goals:

- Minimize disruption to the production environment.

### STEPS FOR DESIGNING THE ACTIVE DIRECTORY ARCHITECTURE

- Design forest, tree, and domain structure: When designing your forest, start with one domain; ensure that additional domains are justified. Keep the domain structure as broad and flat as possible to facilitate faster searches for objects within the directory
- Design the DNS structure and namespace
- Justify any additional forests
- Justify additional Windows 2000 domains
- Justify an explicit trust between domains
- Select domain migration model
- Design domain schema: The schema should be consistent throughout the enterprise for ease of administration. Object definitions within a tree must be consistent; however, definitions can differ between the trees in a forest
- Design site boundaries, *intrasite* replication, *intersite* replication, and site scope: Determine the size of a site and the factors affecting site scope. Services performed within a site include the following: client authentication, group policy execution, global catalog sourcing, domain controller sourcing, replication, DFS access, and file replication services (FRS) that replicate system policies and logon scripts stored in System Volume (SYSVOL) and replicate data for distributed file system
- Design global catalog structure and usage: Design the global catalogs very carefully, specifying attributes that will be indexed for rapid searching
- Design OU structure and determine what justifies the creation of OUs
- Delegate administration
- Design Group Policy Objects (GPOs); that is, site, domains, and organizational units (SDOUs)
- Design site GPOs
- Design domain GPOs
- Design OU GPOs
- Determine GPO overlap for even more granular permissions

Figure 3. Designing Your Active Directory Architecture

- Maintain or improve system performance.
- User access to data, resources, and applications must be maintained during and after the migration.
- The users' familiar environment must be maintained during and after the migration.
- There must be minimal impact on security policy.
- The enterprise must obtain earliest access to key features of the new platform.
- There must be minimal setup of new permissions for resources.
- Administrators should only have to visit the client computer a minimum number of times.
- If possible, users must be able to retain their passwords.
- There must be seamless migration of user accounts.

## Domain Migration Methods

Two basic types of migration scenarios when migrating from a Windows NT Server 4.0 environment to Windows 2000 include domain migration and incremental upgrade or migration.

### Domain Migration

Domain migration provides the most rapid path to migrating to Windows 2000 and the Active Directory. This is an in-place upgrade of your domain. Some high-level steps involved in a domain migration include:

- Take a synchronized backup domain controller (BDC) of the master account domain off-line; this provides a back-out plan.
- Upgrade the primary domain controller (PDC) of the master account domain and at least one BDC.
- Leave at least one BDC as Windows NT Server 4.0 to maintain a mixed-mode environment. Do not switch to native mode (all Windows 2000 domain controllers) until you need some of the replication and scalability that comes with native mode.

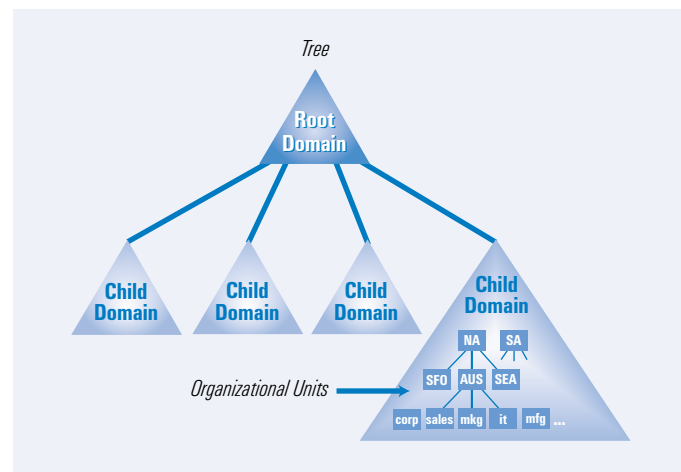


Figure 4. The Organizational Unit Tree Structure

## ACTIVE DIRECTORY FEATURES

**Disk defragmentation utility:** Windows 2000 Server and Windows 2000 Professional support the ability to defragment disk volumes, which are formatted as File Allocation Table (FAT), FAT32, and NTFS.

**Enhanced backup utility:** The Windows 2000 Server Backup utility helps protect data from accidental loss due to hardware or storage media failure. With Windows 2000 Server, the utility can back up data to a wide variety of storage media, such as tape drives, external hard disk drives, zip disks, recordable CD-ROMs, and logical drives.

**Kerberos authentication:** The Kerberos Version 5 authentication protocol replaces Windows NT LAN Manager (NTLM) as the primary security protocol for access to resources within or across Windows 2000 Server domains. Full support for Kerberos Version 5 protocol provides fast, single login to Windows 2000 Server-based enterprise resources, as well as other environments that support this protocol.

**Multimaster replication:** With multimaster replication, changes can be made on any domain controller within the domain. The domain controller then replicates the changes to its replication partners. Using multimaster replication results in 100 percent availability of the directory for changes, even if single domain controllers are unavailable. In addition, by providing multiple copies of the directory across multiple servers, the Windows 2000 Server directory is able to scale to meet enterprise needs.

**Network load balancing:** Network load balancing balances and distributes client connections (Transmission Control Protocol/Internet Protocol, or TCP/IP, connections) over multiple servers—such as Web, proxy, or file transfer protocol (FTP) servers—scaling the performance of TCP/IP services as well as ensuring their high availability on any type of server; primarily used for Web and application servers.

**Windows NT File System 5:** Windows 2000 Server includes an enhanced version of the Windows NT File System (NTFS), which offers support for file encryption; the ability to add disk space to an NTFS volume without rebooting; distributed link tracking (which helps to resolve shortcuts and OLE links to NTFS-resident files that have undergone a change in name or path); and per-user disk quotas to monitor and limit disk space use; as well as many performance enhancements.

**Public Key Certificate Server:** X.509-based Public Key Certificate Server and integration with Active Directory allows the use of public-key certificates for authentication. The Public Key Certificate Server built into Windows 2000 Server is for organizations that want to issue public-key certificates to their users without depending on commercial certification authority services.

**Smart card support:** Smart cards are a key component of the public-key infrastructure that Microsoft is integrating into the Windows platform. Smart cards enhance software-only solutions such as client authentication, single sign-on, secure storage, and system administration.

**Windows Installer Service:** This provides complete reliable software installation and maintenance services to reduce dynamic link library (DLL) conflicts and enable better management of desktop applications.

**Windows NTLM:** The NTLM protocol was the default for network authentication in the Windows NT Server 4.0 operating system. It is retained in Windows 2000 for compatibility with down-level clients and servers. NTLM is also used to authenticate logons to stand-alone computers with Windows 2000.

**Windows Scripting Host (WSH):** The WSH allows administrators and users to save time by automating many user interface actions, such as creating a shortcut, connecting to a network server, disconnecting from a network server, and so forth.

---

*The Active Directory uses the Domain Name System (DNS) as its locator service, organizes objects within domains into a hierarchy of organizational units (OUs), and allows multiple domains to be connected into a tree structure.*

---

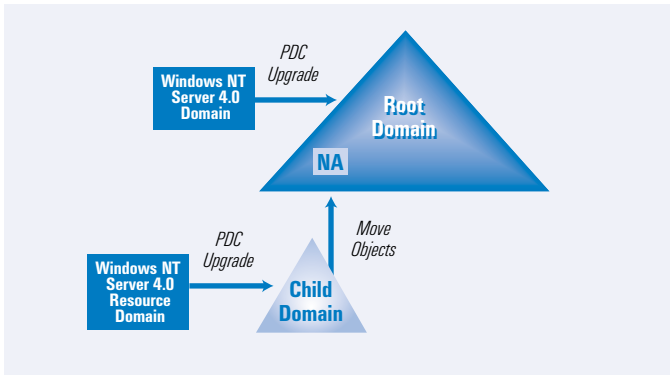


Figure 5. Primary Domain Controller Upgrade

- Next, proceed with upgrading all resource domains using the same steps as above.
- Move objects from new Windows 2000 domains to the upgraded account domain and organize as needed. After all objects have been moved out of the Windows 2000 resource domains, retire the resource domains.

Figure 5 shows the primary domain controller upgrade.

### Incremental Migration

Incremental migration is more suitable for companies that need to completely redesign their systems and domain structure. However, this method also requires additional hardware for the migration. A high-level description of an incremental migration (see Figure 6) includes:

- Create the new forest or root domain by performing a clean Windows 2000 install.
- Establish down-level trusts between established Windows 2000 domains and the original Windows NT Server 4.0 domains so that moved users can access the resources.
- Clone groups and users by using the ClonePrincipal utility (provided in Windows 2000); this will create a duplicate user in the new domain.
- Move computers using the NetDom utility (provided in Windows 2000) to join the computers to the new domain.
- Once all users, groups, and resources have been moved or copied, retire the Windows NT Server 4.0 domains by taking any remaining Windows NT Server 4.0 controllers off-line and remove trusts.
- Decommission the Windows NT Server 4.0 domains.

### Deployment Methods to Consider

The right deployment method will depend on your local IT policies and supporting infrastructure. Microsoft has improved existing deployment methods and has included new ones.

**Unattended Installs.** Microsoft has substantially improved the unattended install by creating a wizard-based setup manager that guides you through the process

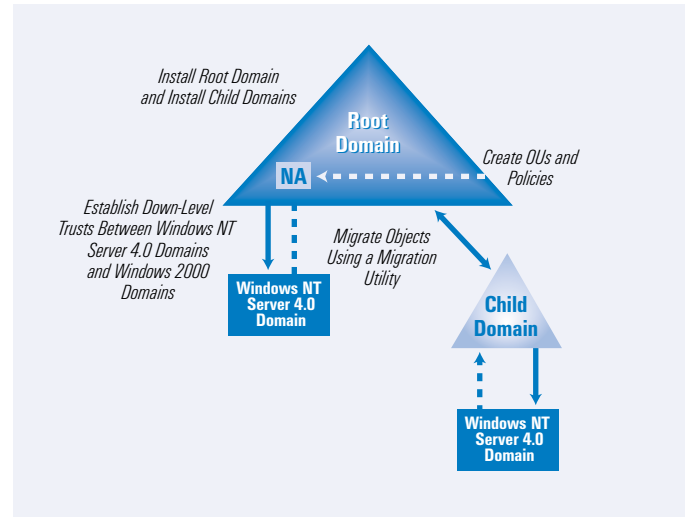


Figure 6. Migrating Objects Using a Migration Utility

of creating the unattend.txt file for hands-free installation. The setup manager runs across the network and is the most flexible method of deployment automation. Use an answer file to specify settings that are common to multiple computers and use a uniqueness database file (UDF) during an unattended installation to identify unique settings to a computer.

**Duplication.** When deploying a large number of computers on identical hardware, you can use the duplication method through the Sysprep tool (sysprep.exe), which prepares the disk for duplications. Storage controllers, hardware abstraction layers (HALs), and advanced configuration and power interface (ACPI) functionality must all be identical. Sysprep allows you to set up and configure the computer and duplicate the hard drive for deployment. It strips the Security ID (SID) from the computer, but when the computer is rebooted, it regenerates the SID.

**Remote Installation Services.** New to Windows 2000, Remote Installation Services (RIS) allows the installation of Windows 2000 on client computers. RIS uses dynamic host configuration protocol (DHCP), DNS, the Active Directory, and the Preboot Execution Environment (PXE)-enabled client for policy-based installation. The PXE client, using DHCP, makes the request for the install service. Combining RIS with IntelliMirror® can provide a completely unattended installation and user settings. ♦

*Linda Chapman (linda\_chapman@dell.com) is the senior product marketing manager for Microsoft OS at Dell Computer Corporation. Linda has worked with Dell IT as a global Windows NT architect. She has also been an independent consultant specializing in Windows NT migrations for Fortune 500 companies. She is an IT programmer, network engineer, and a Microsoft Certified Systems Engineer (MCSE).*