Migration to Windows 2000 Active Directory - Planning and Strategy

While a directory service is not a new concept in the world of network technology, Active Directory represents a major enhancement to Microsoft's new network operating system – Windows 2000. The Windows 2000 line of server products represents a powerful and robust operating system that presents many new features. The most significant enhancement is Active Directory.

What is a Directory Service?

Think of a **directory** as a phone book – with names of people, and their addresses and phone numbers. A network directory can also contain names and addresses, but also a lot more information. Information within a network directory is organized as objects. There can be many different types of objects, such as users and printers. Every resource on the network is stored as an Object in the directory. So, while the directory is the information repository, the **service** is the component that organizes the repository into a logical and accessible structure.

Unlike Windows NT 4.0, Windows 2000 offers the ability to store information about your network (devices, users, and services) in a specialized, central repository that is structured in a hierarchical format. In most networked environments today, information about people, applications, and resources is scattered throughout different databases, or proprietary directories. A centralized, structured, and indexed repository makes resources easier to find, manage, and use. Active Directory is also the most challenging piece of a Windows 2000 migration

There are multiple steps to take into account when planning and conducting a successful migration- a simple in-place upgrade should not be expected for large environments. Before any planning occurs, you should have a firm understanding of Active Directory's core components. It is important to have a thorough understanding of these elements in order to effectively design an Active Directory structure.

Active Directory is built upon several core components divided along physical and logical concepts In Active Directory resources are organized in a logical structure that mirrors the logical structure of your organization. Grouping resources logically enables you to find a resource by its name rather than by its physical location. Because you group resources logically, Active Directory makes the network's physical structure transparent to users, making information easier to locate and use.

Start by learning about the logical concepts of the directory – Namespace, Schema, Domains, Organizational Units, and Forests – which affect how information is stored, and subsequently accessed by your users. To begin with, learn how the components relate to each other to store information. Learn how specific pieces of information can be stored in Active Directory; and all information is stored as objects. The directory schema defines the type of information that can be stored, and the corresponding objects that represent the information in the directory.

Did you know that Windows 2000 can be deployed without Active Directory, but Active Directory cannot be implemented without the Windows 2000 operating system?

Most of the benefits of Windows 2000 are predicated on the deployment of Active Directory; however, Microsoft realized that there must be a way for Windows 2000 to coexist with NT 4.0 in the same environment. So they designed two modes of operation for Windows 2000, one for a pure Windows 2000 environment (native mode), and one for a mixed-environment (mixed mode) where NT 4.0 and Windows 2000 domain controllers can be members of the same domain.
Without the option of deploying Windows 2000 without Active Directory, NT 4.0 domain controllers would not function with Windows 2000 domain controllers because NT 4.0 is not capable of supporting a few key enhancements that Windows 2000 offers in native mode – such as group nesting, automatic two-way transitive trusts, and a larger security database.

To facilitate user access, objects in the directory are located by the Domain Name Service (DNS), which identifies objects by a unique name. Together with other object names, a namespace is formed. The namespace is used to locate the position of objects contained in Domains within the directory. All of the objects in the directory are stored in Domains that act as boundaries for key functions such as authentication, administration, and replication. Organizational units are used to organize objects within a Domain more efficiently and effectively. All of the Domains that share a common schema comprise a Forest. A Forest enables communication between of the domains, and forms an enterprise directory.

Once you understand how information in the directory is stored, learn about the physical concepts –Replication, Sites, and a Global Catalog – that determine how directory information is distributed in networked environment. Users and services should be able to access directory information at any time from any domain in a Forest. Replication ensures that the latest information is always made available to your users. The speed of your network will affect the replication of the directory information.

Active Directory distinguishes between fast, and slow links for efficient replication through the creation of Sites. A site is a combination of one, or more Internet Protocol (IP) subnet connected by a highly reliable and fast link to localize as much network traffic as possible. Because a fast link is present, Directory information within a site replicated more frequently than information between sites. The fast links also provide optimal login conditions for Active Directory clients, who will preferentially login to a domain controller within their site (on the same IP subnet). Directory information is replicated to domain controllers both within and among sites; however, a Global Catalog

server provides the most common information about all of the objects within a directory. Just as a directory is analogous to phone book, a Global Catalog server is just like a speed dialer that provides directory clients with object information from anywhere in the directory the fastest way.

Again, how well you understand Active Directory will greatly affect your ability to design a sound directory structure. When entering the directory design phase of your project, remember to start simple – only add components to your directory unless there is a qualifying reason.
Active Directory design deals as much with human issues as with technical issues. The ideal design team consists of several decision makers who have a strong knowledge of the company and authority to make binding commitments for those that they represent, at least one technical expert in Active Directory, and an overall project manager.

Each of the core Active Directory components – forests, sites, domains, and organizational units – addresses different facets of a unified directory service. Each new forest, site, domain, or OU should be created only if there is a valid technical reason to do so – don't simply mirror your existing network structure. It is helpful to have a framework of decision points to follow, starting with the most important (forests) and ending with the most flexible (Organizational Units).

As with all components, start with a single forest. Implement a new forest only if your organization requires multiple schemas, as might be required with schema-modifying applications. The first domain created in a forest is very important – it holds several key forest roles, and is used as the domain suffix for all user principal names (Bob@MyCompany.tld) in the entire forest. Consider creating a placeholder domain as the forest root, and implementing child domains for the actual company structure. The most important thing to remember when creating your forest plan is that forests are not easily changed after they have been deployed. Forests cannot be merged or split, and domains cannot move between forests.

Create additional parallel domains in the same forest to reflect multiple registered Internet names. Create child domains to represent administrative boundaries, or to represent different domain-wide account policies. You do not need to create separate domains merely to reflect your company's organization of divisions and departments. Within each domain, you can model your organization's management hierarchy for delegation or administration using OUs for this purpose, which will act as logical containers for other objects.

Organizational Units within domains should be implemented to delegate administration, to apply differing Group Policy Objects, or to run differing login scripts. An OU can replace an NT4-style domain during a migration, so consolidation of multiple small NT 4 domains into a single Active Directory is possible. Groups within an OU allow for even more detailed control, and both groups and OU's are easily changed to reflect future company changes.

Guiding Active Directory Design Principles:

- ✓Keep it simple
- ✓Aim for the ideal design
- ✓Evaluate several alternatives
- ✓Anticipate change

An Active Directory domain can span multiple physical locations, if these locations are all administered centrally. Sites are defined to control replication across slow network links. If two domain controllers are connected by a link of less than 512 kbps, creating two different sites will allow intra-domain replication to be scheduled and compressed.

For all features, make the best design decision based on technical merit, allowing for present and future business operations. Examine the decision points for each level and if the rules of Active Directory dictate a new domain, a new site, or a new organization unit, than make it so.