



Windows 2000 Active Directory Design— Dedicated Forest Root

By Peter J. Salmeri & James N. Barrett,
Senior Network Systems Consultants

Introduction

Microsoft's Windows 2000 operating system offers an organization a significant amount of new functionality and design flexibility. However, these benefits do come at a price; design complexity has increased considerably. Historically most users were content to allow Windows NT to grow somewhat organically in their organizations; domains were created for various reasons. Originally, most domains were islands of information. A department or group of users would need the resources of a Windows NT domain, so one was created for them. During this early time of NT adoption, there was no significant need to share domain resources across an enterprise. As time went on, the Windows NT structure grew and users started to require access to resources in other domains. Microsoft answered this need with the ability to have domains "trust each other. Now a user in Marketing could access resources in a Human Resources domain without needing to have an account there.

This new model also worked well for a time, but the system of creating manual trusts between domains can get fairly cumbersome. At about the same time, the pendulum in the information systems arena started to swing the other way and the concept of the centralized IT department enjoyed a rebirth. This return to the philosophy of centralized management conflicted somewhat with the design of Windows NT. NT was designed to allow independent administrators to control their resources and users, utilizing the trust model to permit or deny outside users. . Basically, Windows NT was poorly suited to the concept of centralized control, especially for a large number of domains.

Microsoft saw this change beginning several years ago and decided to address it in the next version of Windows NT. As promised, this issue has been fully addressed in Windows 2000. Domains in an organization are part of a larger unit called a forest. Within the forest, trusts between domains are automatically created and maintained and a centralized administration group—the Enterprise Administrators group—is utilized to give a central IT structure the ability to control all domains in the forest from a centralized point. At the heart of Windows 2000 is the Active Directory, the distributed database that controls all aspects of the operating system.

Creating an optimal Active Directory (AD) design is a challenging task that should not be taken lightly. During the design process, Active Directory architects must balance business and technical considerations to develop a design that reflects an organization's unique requirements. These architects can incorporate a number of design techniques, such as the *Dedicated Forest Root*, that can provide additional levels of security, administrative access control, and flexibility. This paper deals specifically with the concept of the Dedicated Forest Root.

The *root domain* is the term used to describe the first domain installed in a forest. Since it acts as the “root” of a Windows 2000 Active Directory structure, it has certain functions and abilities that set it apart from all of the other domains in the tree. For example, the root domain contains two security groups, the Schema Administrator group and the Enterprise Administrator group, that do not exist in any other domains within the Active Directory forest. Both of these groups have the ability to make forest-wide changes, such as the addition of new domains to the forest or modifications to the forest schema.

A *Dedicated Forest Root* is a root domain that serves as a placeholder; it does not contain user or computer accounts. Instead, administrators reserve the Dedicated Forest Root domain to contain only the default, built-in administrative accounts and groups. (It is important to note that there is no technical difference between a forest root domain and a Dedicated Forest Root, other than the fact that the administrators have chosen not to place user and group accounts in the root. Instead, they place the users, groups, and computer accounts in other domains in the Active Directory forest.)

A Dedicated Forest Root is intended to enhance the flexibility and security of the Active Directory design, as well as alleviate potential political issues that could arise due to the power inherent in the special administrative groups of the root domain.

As Windows 2000 becomes widely accepted by the corporate world, many companies will be faced with questions regarding forest administration rights and will want to understand some of the design options available. This whitepaper has been written to help such companies weigh the benefits and drawbacks of the Dedicated Forest Root concept.

Dedicated Forest Root Benefits

The benefits of the Dedicated Forest Root can be summarized as follows:

- Increased control of schema changes and modifications
- Increased control over actions that impact an entire Active Directory forest
- Improved design flexibility

Let’s examine each of these benefits in more detail.

Improved Schema Security

As mentioned earlier, the root domain houses two unique security groups that have the ability to modify several important forest-wide settings. One of these groups is the Schema Administrators group, which has the ability to control the Active Directory schema.

The Active Directory schema is a data store that contains definitions of object classes and the attributes that can be utilized in an Active Directory forest. An object class defines all of the properties that can be associated with a particular object. For example, the user “jsmith” is an object. The log-in name, full name, description, password, etc., are all attributes of jsmith’s user object. The object class “user” contains the listing of all of the possible attributes that can be associated with a user object.

One of the features of Active Directory is an extensible schema, which means that the schema can be modified to suit the requirements of an organization. For example, new attributes can be added to an object class. To continue the previous example, many companies assign an identification number to their employees. A company could extend the existing schema to add an attribute called

“HR ID” to the user object class. Now, an additional piece of information exists for each user that can be edited, sorted on, etc.

By default, the Active Directory installs with approximately 120 object classes and about 800 attributes. However, many directory-enabled applications add new object classes and attributes to the schema. For example, Exchange 2000 will add approximately 150 object classes and more than 800 additional attributes when it is installed into an Active Directory forest. As these attributes become populated, the amount of replication traffic traversing the network will grow. For this reason, changes to the Active Directory Schema need to be closely monitored.

Once a change is made to the schema, it can be deactivated, but cannot be removed. For this reason, it is imperative that schema changes be planned and executed with the utmost care.

In order to modify the schema, a user must be a member of the Schema Administrators (SA) group, which resides in the root domain. Organizations, especially large, multidivisional companies, will want to maintain tight control over schema changes. The Dedicated Forest Root provides a mechanism to do this. By separating the Schema Administrators group from other day-to-day security groups, and by restricting the ability to modify membership of the Schema Administrators group, organizations can obtain a much higher level of control over possible schema changes.

Improved Administrative Access Control

Another powerful administrative group found within the root domain is the Enterprise Administrators group. Members of the Enterprise Administrators group have full administrative control over all domains within the forest. By default, the Enterprise Administrators group is added to the Domain Administrators group for each domain in the forest. More importantly, the Enterprise Administrators group is also the only one that is allowed to make changes that affect the forest as a whole, such as the addition or removal of new domains.

A third administrative group to note is the root domain’s own Domain Administrators group. As in any domain, members of the Domain Administrators group have rights to administer all functions within their domain. Since the root domain contains both the Schema Administrators and Enterprise Administrators groups, members of the root Domain Administrators group can modify the membership of these two groups. Although members of the Domain Administrators group do not inherently have the ability to manipulate the schema or administer any other domains, users who are members of the Domain Administrators group can simply add themselves to either the Schema Administrators or Enterprise Administrators groups and gain full rights to the forest. For this reason, it is critical to carefully restrict membership to the Domain Administrators group in the forest root domain. By utilizing a Dedicated Forest Root, organizations can maintain tight controls over Domain Administrators group membership.

Improved Design Flexibility

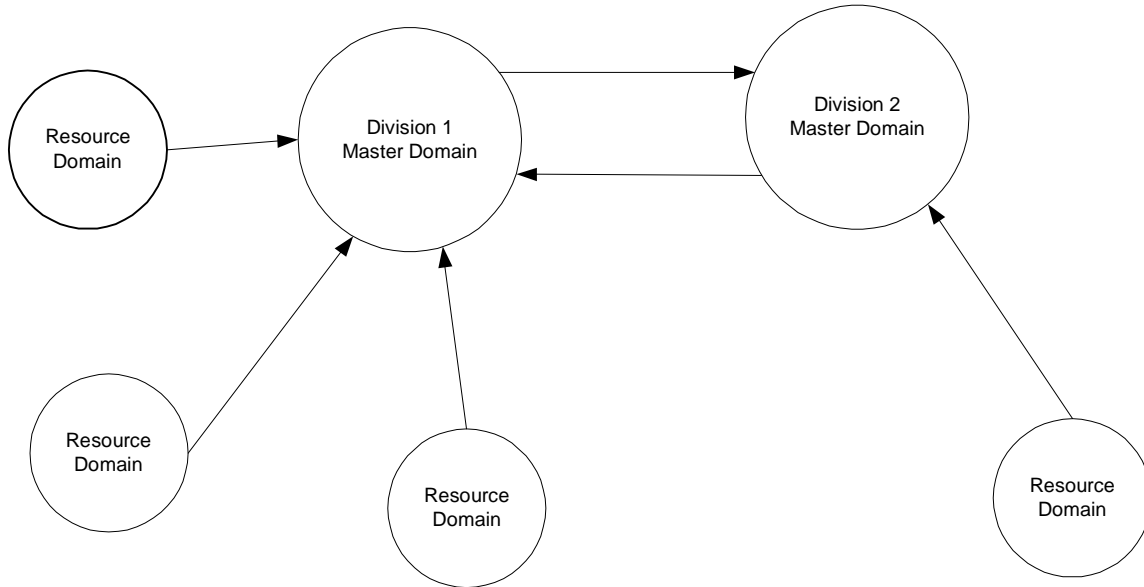
It is important to design an Active Directory structure that can be easily maintained throughout acquisitions, mergers, and divestitures. Use of the Dedicated Forest Root in the design permits flexibility for reconfiguration in the future.

This concept is best explained by an example. XYZ Corporation currently has an NT4 domain structure. We have been asked to assist it with an upgrade to Windows 2000. The first step is to design its Active Directory structure. XYZ currently has two divisions and is in negotiations to

acquire two new companies during the next year. It also has one under-performing division that is likely to be sold off sometime within the next two years.

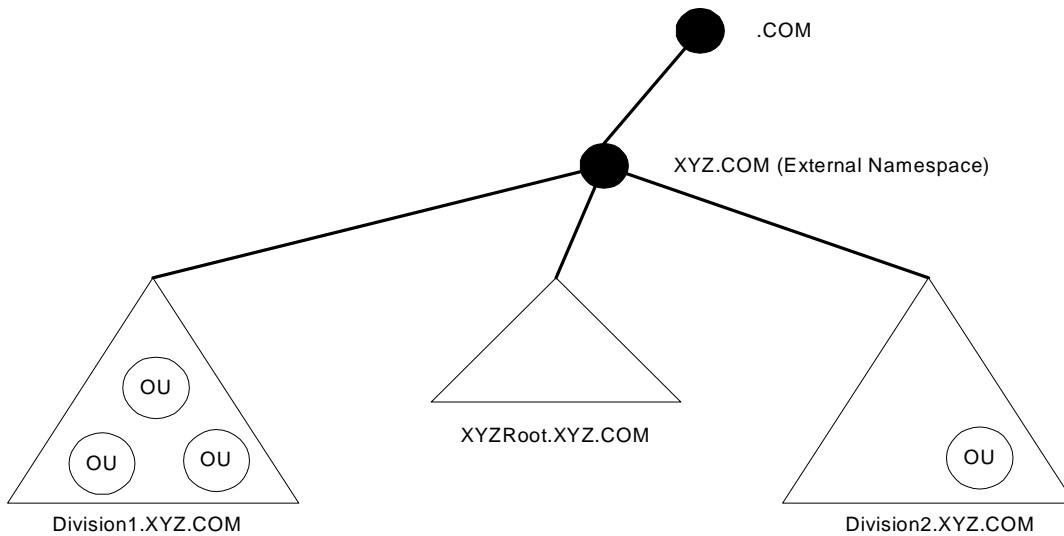
The current Windows NT 4 domain structure looks like this:

XYZ Corporation - NT 4.0



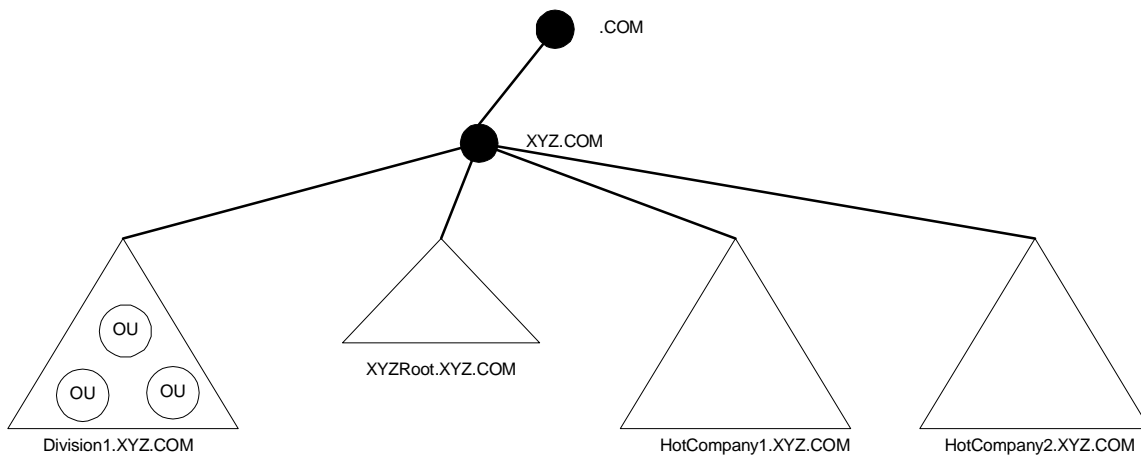
One possible Active Directory design would be to create a single domain and utilize organizational units and administrative delegation to organize resources and permissions. However, this approach would provide very little flexibility: all changes would occur in a single domain, and situations such as mergers, or the divestiture of the under-performing business unit, would have significant and long-lasting impact.

By utilizing the Dedicated Forest Root approach, XYZ Corporation can gain a higher level of flexibility for the addition or removal of business units from the Active Directory forest. In this situation, the root domain will be named XYZRoot. Note that we have chosen not to populate this domain—it is a Dedicated Forest Root. Each of the divisions has been upgraded to Windows 2000 domains. We decided to keep the divisions as separate domains due to XYZ's plans to eventually divest Division 2. The resource domains have been incorporated as Organization Units (OU) into their respective parent domains.



The Dedicated Forest Root domain XYZRoot.XYZ.COM houses both the Enterprise Administrators and the Schema Administrators groups. The Domain Administrators in Division 1 and Division 2 have authority only in their respective domains. This serves the dual purpose of helping to alleviate security concerns and limiting access to the schema to those who have been specifically selected to maintain it. A good change control process should be developed for schema changes.

Once XYZ Corporation acquires the two companies and divests Division 2, the Active Directory can easily evolve without ever changing its administrative model.



The newly acquired companies can continue to administer themselves. Division2 is easily removed from the tree. Had Division 2's domain been the root domain, a clean divestiture would have been impossible.

Dedicated Forest Root Disadvantages

Each domain installed in a forest requires at least one Domain Controller (DC). For redundancy purposes, it is highly recommended that there be multiple DCs per domain. The most obvious disadvantage to the Dedicated Forest Root is the cost incurred in buying the additional servers

necessary to act as domain controllers. For example, if a company's AD design called for two "active" domains and the company wished to use a Dedicated Forest Root, it would actually need to purchase equipment for three domains (the Dedicated Forest Root plus the two "active" domains). In addition to the cost of purchasing the hardware, there are additional administrative and maintenance costs associated with the additional domain. For this reason, many smaller companies may conclude that the benefits received from the Dedicated Forest Root concept do not outweigh the costs.

It is essential to have DC redundancy in the root domain whether the Dedicated Forest Root is used or not. The root domain houses critical forest functions as well as serving as the base upon which the rest of the forest is built. If the root domain is housed solely on a single DC and that DC fails, recovery operations can be very complex and time consuming, because restoration from backup is the only option. It is not wise to rely upon backup tapes alone for such a critical forest function.

Conclusion

The Dedicated Forest Root design affords tight schema control, better delegation of administrative access, and significant design flexibility. These benefits come at the cost of additional hardware and administrative overhead. It is the task of Active Directory designers to weigh the costs and benefits of employing the Dedicated Forest Root and determine if it is appropriate for their organizations.

For further information, see the Lucent NetworkCareSM Professional Services (Lucent NPS) website at <http://www.lucent-networkcare.com>, or call 1-877-369-1115 in the U.S. or 1-727-217-2303 outside the U.S.

NetworkCare is a servicemark and "The knowledge behind the network" is a registered trademark of Lucent Technologies Inc. All other trademarks and registered trademarks are properties of their respective holders.

Copyright © 2000, Lucent Technologies Inc. All rights reserved.