

# ***Upgrading from NT Domains to Active Directory***

## *A Systematic Approach*

Bruce Greenblatt

Directory Tools and Application Services, Inc.

One of the most popular, and unfortunately, most difficult tasks for the network administrator of the 21<sup>st</sup> century is upgrading a network of NT 4 Domain Controllers to Active Directory Domain Controllers. There are several approaches that are available in accomplishing this task. The most obvious one is as follows. On each of the NT 4 Domain Controllers, upgrade the NT 4 Server operating system to some version of Windows 2000 Server (*e.g.* Server or Advanced Server). This is an excellent approach for small organizations with only one domain.

For larger organizations with numerous separate domain controllers, this is normally an unwise approach. This approach does not take advantage of the enhanced capabilities of Active Directory as a centralized repository for the organizations users and computing infrastructure. The best approach is to gradually migrate the numerous separate NT Domain Controllers into a single cohesive Active Directory infrastructure. This is not to say that there only needs to be one Active Directory Domain Controller in the network. However, it is likely that a network of any size can be effectively managed with many fewer Active Directory Domain Controllers than could be possible by continuing to use NT 4 Domain Controllers.

One of the features of Active Directory that Microsoft has provided is the DCPROMO (Domain Controller PROMotion) utility. DCPROMO will turn a member server into an Active Directory Domain Controller. For a machine that is already an NT 4 Domain Controller, the upgrade from NT4 Server to the appropriate version from the Windows 2000 Server family, the upgrade to Windows 2000 will have the option to convert it to an Active Directory Domain Controller. While Microsoft has provided an excellent utility that makes it very easy to move into the Active Directory world, the upgrade to an Active Directory Domain Controller must be used with caution, especially in networks with many domains. One of the reasons for caution is that it is common for the same real world user to be represented by user entries in many separate Domains in an NT 4 based network. It is likely that the naïve approach to the upgrade will result in several different entries in Active Directory for the same real world user. A cautious approach to upgrade is more appropriate to ensure that each real world user is represented by exactly one Active Directory entry.

In a large enterprise, there may be numerous NT4 Domains that need to be upgraded. Thus, the same user may be represented in many domains. Ideally, after the upgrade cycle, there is only one Active Directory user entry for this user. If the upgrade to Active Directory is done in a naïve manner, the Active Directory tree will have one domain context for each NT4 domain that existed prior to the upgrade cycle. These domain contexts are a useless artifact, and should be avoided, as they complicate access control and user administration. Furthermore, the computer objects in these domains will be transferred to the new domain contexts. This is also a problem because Active Directory

will normally be integrated with DNS in such a way that the domain contexts map one to one with the DNS zones. The best scenario is to end up with a single DNS zone, but the upgrade does not provide a mechanism for accomplishing this. For large multi-site enterprises, the best result is to divide the Active Directory domain controllers among various *sites*. See the section below for more information on this new feature of Active Directory.

One of the things that the upgrade process does is preserve the access control and other security information for users, computers, printers, *etc.* from the NT 4 Domains into the corresponding entries that are created in Active Directory. One problem that is common in the upgrade cycle is that many of the servers that are running as NT 4 Domain Controllers are not suitable to run as Windows 2000 Active Directory Domain Controllers.

For computers that are to be used as Active Directory Domain Controllers, a moderate server should have the following characteristics:

- Fault tolerant disk subsystems (multi-disk RAID-5 is best)
  - Size depends on number of users, computers, *etc.*
  - Is the computer to be used as a print server or file server
- Fast Pentium III processor (over 1Ghz, Pentium IV is better)
- Single CPU is OK if other applications are not running on the server
  - Note that we recommend not using a Domain Controller as an Application Server. Application Servers and Database servers can negatively impact the performance of the Domain Controller. Normally the Domain Controller will also server as a DHCP server and a DNS Server. In small enterprises, the Domain Controller often serves as a router for the internal network as well.
  - This means that Advanced Server is not required

A recommended scenario is to upgrade the NT4 Domain Controller to a Windows 2000 Domain Controller, and place the NT4 domain into a new domain context of an existing Active Directory tree as part of the upgrade process. Once this is complete, the NT4 Domain database information has been replicated into the Active Directory the obsolete machine can be retired. If many NT4 machines need to be upgraded in this manner, the same Windows 2000 Server license can be reused as often as required, as long as the obsolete machines are retired from service after the upgrade cycle.

A significant difference between the NT 4 Domain Controller environment and the Active Directory Domain Controller is the type of information that can be stored in the directory. In an NT 4 Domain Controller the information is limited to users, computers (normally only servers, but often includes workstations as well), printers and groups. Also stored as properties of these objects is access control information. The information that can be stored in an Active Directory Domain Controller includes all of the above information plus much more. For example, many modern network devices (*e.g.* Cisco routers) make use of the definitions of the Directory Enabled Networking (DEN)

initiative to allow for remote management of these devices. Similarly, many LDAP-enabled applications, such as Oblix's XXXNetworkSecurityXXX, and Arkivio's auto-stor are designed to work with Active Directory.

Active Directory allows the administrator to divide the network up into WAN-connected *Sites*. Exchange administrators may be familiar with the site concept as it is used in Exchange email networks to control the flow of email among the MTAs. Each site will have one or more Domain Controllers. Directory information that is common amongst Domain Controllers that are in different sites is synchronized differently than is information amongst Domain Controllers that are all in the same site. NT 4 Domain Controllers had no way to limit synchronization traffic between Domain Controllers for a domain that was spread across multiple sites. This lead many administrators to artificially create separate domains for different sites so as to limit expensive WAN traffic that was caused by directory synchronization.

## ***DTASI Tools***

As part of our toolkit, DTASI provides several tools that we use in the migration from NT4 domains to Active Directory.

- **FindUsers:** This utility analyzes an NT4 Domain, and compares the domain users to the ones in Active Directory to find the ones that appear to be duplicates. These duplicate users should be “merged” after the NT4 domain information has been uploaded into Active Directory.
- **MergeUsers:** This utility combines the access control information of two users into one of the users that is designated as the target. Additionally, any group memberships are also combined. This is especially important for mailing list memberships that are maintained within Active Directory.
- **MoveComputers:** This utility moves computer objects from one domain context to another, and also cleans up the DNS information (if possible).
- **CleanDomainContexts:** This utility searches Active Directory for empty domain contexts which should be pruned from the Active Directory tree.