Lucent NPS
The knowledge behind the network

Lucent Technologies
Bell Labs Innovations



Windows 2000 Active Directory Design: Restricting the Enterprise Administrators Group

By James Barrett, Senior Network Systems Consultant

Introduction

Windows 2000 offers an entirely new paradigm to the design of a domain hierarchy. In previous versions of Windows NT, each domain was a virtual island. If users wished to access resources in different domains, a complex system of manual trusts was necessary to facilitate this. As organizations have grown, domain design requirements have become more complex. The system of manual trusts has grown rather cumbersome, particularly for organizations that have dozens or hundreds of domains.

To address these issues, Windows 2000 has introduced the concepts of forests and trees–both of which are collections of domains. A tree is the population of domains that share a contiguous name space. In a tree of three domains, the top domain might have the DNS name of lucent.com. Lucent.com might have two child domains named sales.lucent.com and production.lucent.com. Since all three of these domains share the contiguous name space of lucent.com, they are considered to be part of a single tree. A forest is defined as the entire population of domains that share a common root domain; it can contain a single tree or multiple ones. So for example, a domain might be called nps.com. It is part of the same forest as lucent.com but does not share the same namespace. However, lucent.com was the first domain created in our forest, thus it is the root domain for all other domains that we create in this forest.

There are many advantages to having domains grouped into a forest. First and foremost, the Windows 2000 Active Directory automatically manages inter-domain trusts within a forest. A second major advantage is that tools exist from both Microsoft and third parties to permit the movement of certain types of objects, such as user or computer accounts, from one domain to another in the same forest. A third advantage is a unified administrative model: a user can be designated an Enterprise Administrator (EA) and granted administrative rights to all domains in the forest.

This third feature has caused some controversy; specifically, some organizations want to have a fully segregated domain design such that an administrator in one domain cannot interfere with another domain. This has led some organizations to consider creating separate forests. Separate forests, while they do solve the problem of overlapping administration introduce other complications into the mix; trusts between domains from different forests must be manually managed. If the organization employs Exchange 2000, a common global address book is not possible since the address book is defined on a forest basis. Finally, the ability to move user and computer objects between domains is lost since no tool currently exists to move an object from one forest to another.

Fortunately, if an organization wants to achieve this kind of administrative separation, there is an alternative to creating multiple forests: blocking the EA group from accessing a particular domain. This paper demonstrates how an organization can leverage the benefits of the single forest model while still retaining the security independence of the multiple forest model.

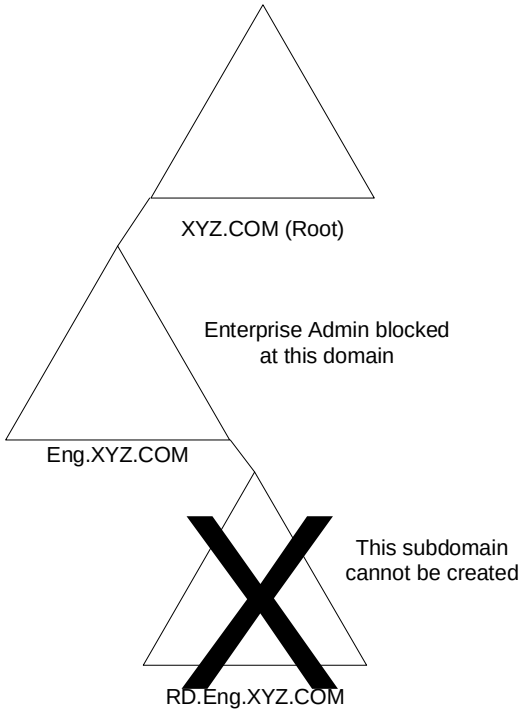
Using a single forest model in an organization offers several advantages:

- One forest is easier to administer than multiple ones.
- An organization can maintain a much tighter degree of control over a forest if items such as structure and schema are centrally managed.
- A common global catalog speeds searches.
- A common e-mail directory makes it much easier to unify messaging across the company. For example, Exchange 2000 utilizes the global catalog to generate the Global Address List. The global catalog has the forest as its boundaries.
- Multiple forests require manual administration of trust relationships between forests. One of the reasons to migrate to Windows 2000 is to make use of transitive trusts and minimize with manual trust configuration and troubleshooting.

For some companies, clearly defined security boundaries are more important than ease of administration or common e-mail directories. At first glance, these organizations might conclude that the best model is a multiple forest one, with sensitive information placed into its own forest and administered solely by the owners of that data. Although this is certainly a viable solution, an alternative exists. It is possible to leverage the benefits provided in the single forest model, while at the same time allow a domain to cut itself off administratively from the rest of the forest. Since the EA group is the only forest group that has the rights to administer all objects in that forest, the key to creating clear administrative separation is to take measures to remove the permissions of the EA group at appropriate domain boundaries.

Issues with EA Restriction

There are a number of repercussions that arise from removing the EA from a domain. For example, the creation of sub-domains will be restricted. To illustrate this, the EA has been blocked from the Engineering domain in the following example. It is now impossible to add any sub-domains to Engineering. Remember that in order to add a sub-domain, a user must have domain administration rights in the parent domain in addition to full administration rights to the Active Directory. Normally, the EA group is the only object with sufficient rights to perform this task. Since the EA has been denied rights to Eng.XYZ.COM, the parent domain, no object in the tree has sufficient rights to create RD.Eng.XYZ.COM.



New sub-domains cannot be created, so it stands to reason that existing ones cannot be deleted either. Therefore, the tree structure below a blocked domain cannot be changed by anyone unless administrative rights are restored to the EA group.

Another important responsibility of the EA group is DHCP server authorization. To authorize a DHCP server, two requirements must be met. First, a user must have administrative rights in the root domain. Second, a user must have rights to see the DHCP server in the target domain. By default, only users who are members of the EA group satisfy both of these requirements. It is possible to revoke EA rights in a domain, but still give the EA the right to authorize a DHCP server. The EA can be made a member of either the DHCP users group or the DHCP administrators group in the local domain. If these rights are granted, the EA now can "see" the DHCP server in the target domain and has sufficient rights to the Active Directory to authorize the DHCP server. Note that a Domain Administrator in the root domain could be similarly granted the right to authorize DHCP servers using this procedure. Any user that meets the two requirements stated above can authorize DHCP servers.

If an organization chooses to exclude the EA from a particular domain, it is possible to re-grant the EA rights to that domain at a later date by simply reversing the steps that were taken to remove it. This would enable an organization to make changes that require EA authority and then remove the EA once again to restore security.

Danger: Administrative Lockout

At this point, an interesting question comes to mind: If the local domain administrator can eject the EA from the local domain, what stops the Domain Administrator from doing that without authorization? The short answer is: nothing. Windows 2000 has inherited many aspects from its predecessors–one of which is the philosophy that the local administrator has ultimate authority in their domain. A local administrator has the right to determine what goes on in their domain and can

grant or deny others rights at their choosing. For this reason, it is wise to be very careful who is granted domain administration authority since this person has the ability to cause a lot of damage to the network.

Removing the EA from the Domain: Exact Steps

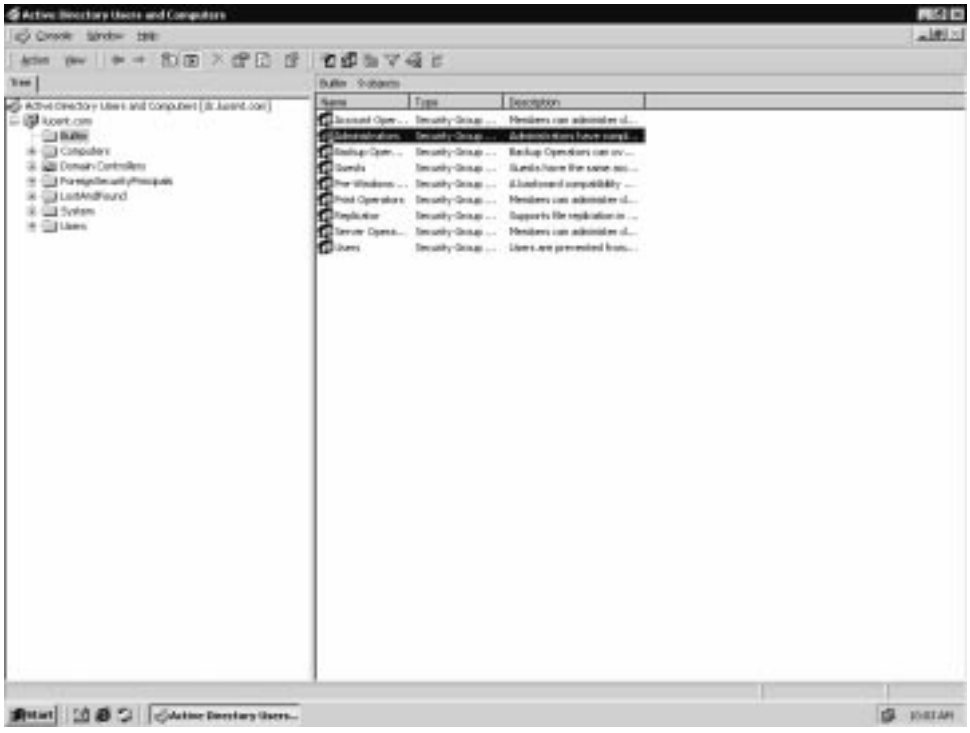
Given the problems that can occur if an EA is removed from a domain, Microsoft has made it more complicated to eject the EA from a domain than by simply revoking rights. Three steps must be taken to fully isolate a domain from EA control. The EA must be removed from the local domain administrator's group and have their rights revoked to the domain object. As a final precaution, by default the EA has rights to each domain's local administrator object, which would permit the EA to change the password and use that account to access the domain if the EA were otherwise cut off. These rights must also be revoked to ensure security.

The following steps describe how to remove the EA's authority from a particular domain.

Note: While the author performed testing necessary to explore this concept, he did not test the long-term ramifications of following these procedures to block the EA. The user is cautioned to perform proper testing before employing this methodology in a production environment. The author assumes no responsibility for any complications that result from these procedures.

Step 1: Remove the EA from the Local Domain Administrators Group

Choose the domain in which you wish to restrict the EA. Right click on the Administrators group and choose properties, as shown in the following screen shot.

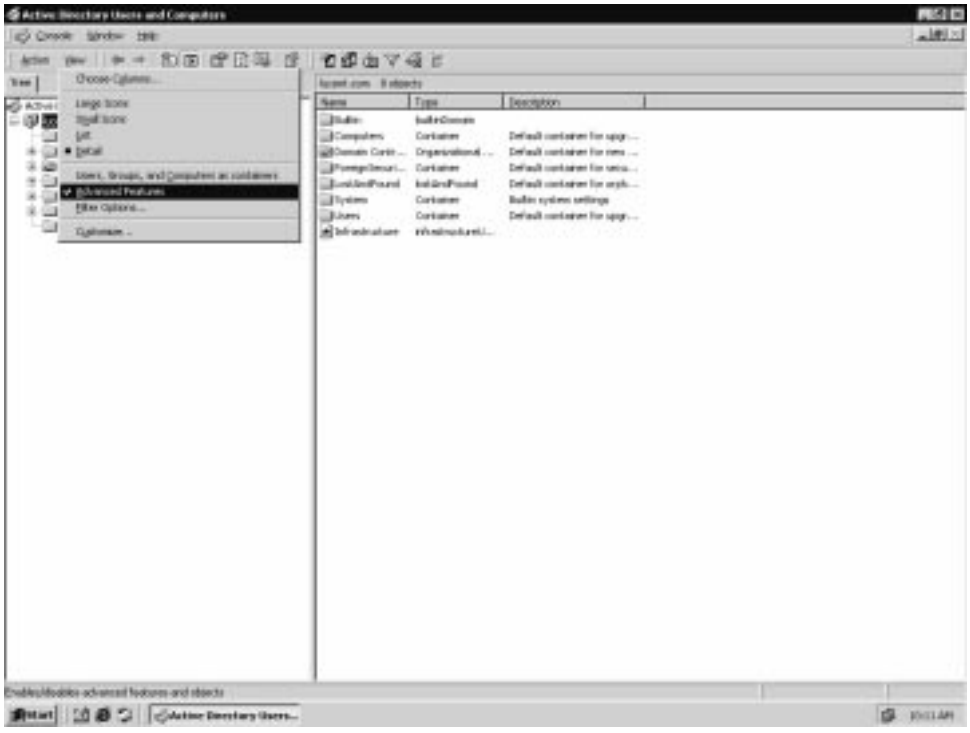


Then, select the Members tab and delete the EA group.

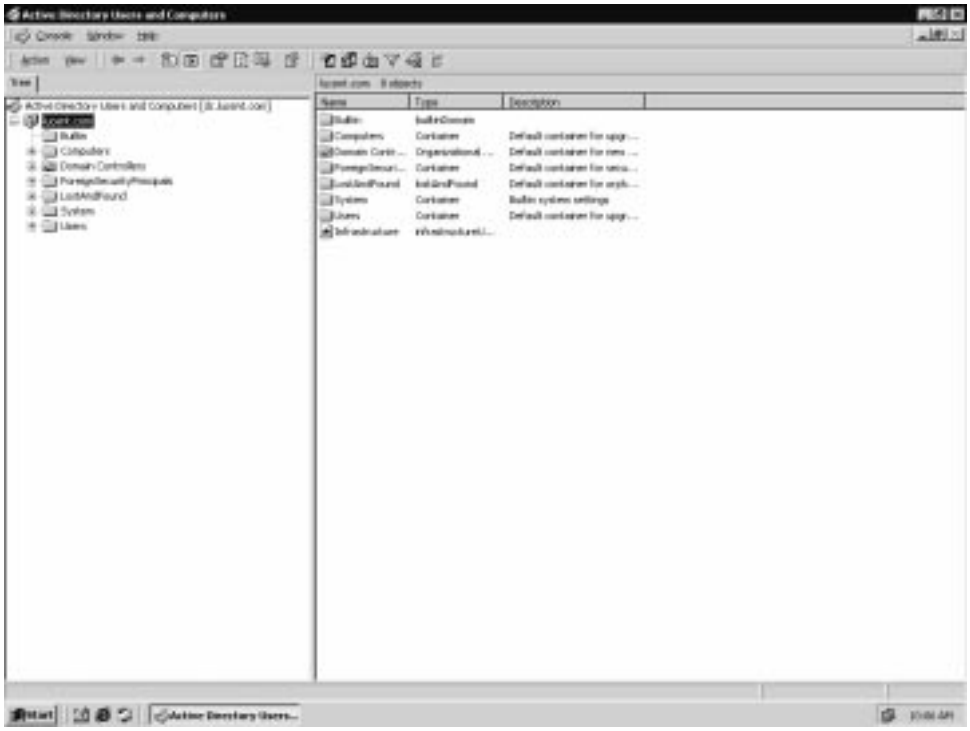


Step 2: Remove the EA's Rights to the Root Object

Select the Advanced properties setting from the View menu.



Then, right click on the target domain's root object and select Properties.



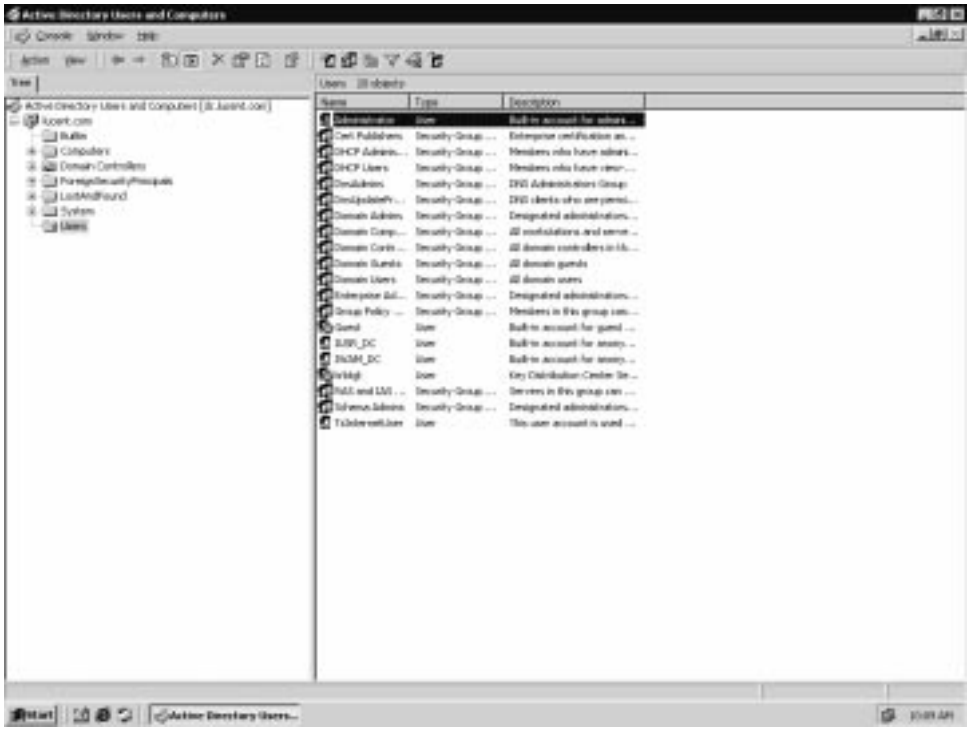
Select the security tab and remove the EA's permissions from the list.



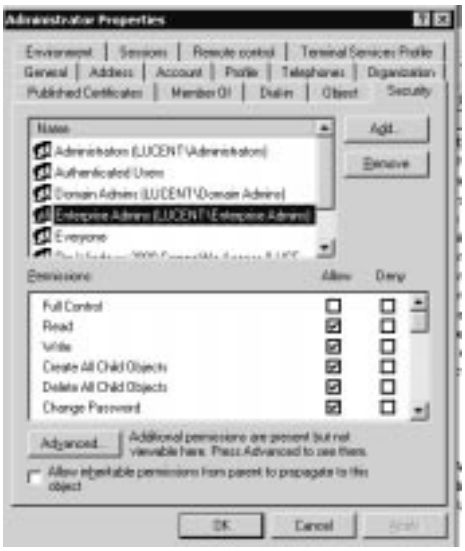
Step 3: Remove the EA's Permissions from the Local Administrator

As a final failsafe, the EA group is granted rights to each local Domain's Administrator object. The enables an EA to change the password, etc. It is necessary to block the EA's rights to this object to completely partition the domain.

Right click on the default Administrator account and select properties.



Then, select the security tab, and remove the permissions for the EAs.



At this point, the EA has been completely blocked from the domain.

Summary

In summary, it is possible to achieve the goal of administrative separation while at the same time not give up the advantages of a single forest. The purpose of this paper has been to show the mechanics necessary to block the administrative rights to a domain that the EA group has by default, while at the same time making the reader aware of some of the ramifications involved should this be attempted.

There is an alternative to blocking the EA group–a dedicated forest root domain. I have co-authored another whitepaper, which describes this concept in greater detail, but the basic concept is to create a root domain that has minimal objects. It is primarily intended to serve as a placeholder domain and all other domains are either created underneath it in a single tree or as part of other trees. The intention would be to grant very few people administrative rights to this domain. Since the root domain is the one which houses the EA group, very few users would need to have forest-wide administrative rights.

The methodology that the Windows 2000 designer chooses will be dictated by the corporate environment. In most cases, there really should not be a need to block the EA from a domain. If some separation of responsibility is required; the dedicated forest root is the preferred method of limiting forest-wide administrative access. The only time that one should consider blocking the EA is if the organization has a specific need to completely segregate a user group for reasons such as governmental security classifications or research and development trade secret issues.

For further information, see the Lucent NetworkCare℠ 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.