Securely Maintaining the Integrity of Active Directory

- Vinod Khushaldasani

Companies often do not adequately consider how to maintain the integrity of Active Directory to avoid Active Directory pollution. It is very important to start planning on how to ensure that the data entered is not only accurate and consistent but is also in the correct format.

Active Directory is the most critical database in the enterprise. Compared to the NT SAM database the AD is a much larger database with new classes and fields to maintain now one has to plan the data and format for each field. Yes, one could write pages and pages explaining each field and its contents that may vary by location and by department. What a nightmare it would be, then, to maintain this on a regular basis. Let us say that all this was put in black and white and sent to the local Administrators at each site. Once the document is in their hands, the integrity of the data and adherence to the guidelines is at their mercy.

It is impossible, though, to ensure that the data entered in Active Directory is accurate if it's not enforced. Moreover who has the time, to maintain that document as the enterprise grows or the infrastructure changes? Even if the document is maintained one must also ensure that the local administrators not only receive the updated document and read it but also, follow it. If there is no control over the data entered into the directory, one cannot rely on the Active Directory queries to be accurate. The other requirement would be to have a central robust reporting or tracking mechanism to determine the culprits circumventing the policies. How helpless would one feel to find out that after going through all this pain in maintaining the document it is not being adhered by? How can one securely delegate certain limited administrative tasks without giving too much power to the administrators? If all the administrator needs to perform his duty is manage 3 attributes why give him the power to manage anything more without creating an ACL hell?

Do not spend too many sleepless nights over this. The NetIQ Administration Suite comes to the rescue for all such network administrators. The suite includes Directory and Resource Administrator, which ensures the security of Active Directory by providing granular delegation, preventing escalation of powers, logging and reporting on every administrative function, enforcing policies and automating routine tasks. With all these features DRA increases the security of the enterprise, reduces the workload and increases efficiency.

Delegation

The Delegation of Control Wizard is Microsoft's answer to delegation but is this enough and does it address the real issues that companies face everyday? The Delegation of Control Wizard in Active Directory is restricted in terms of functionality. To get any granular delegation natively the ACL editor must be used. ACLs can only be set on a per object basis and there is no way to report on them. There is also no way to tell who has what permissions set and over which objects. If one has a large environment or a constantly changing infrastructure the ACL editor is impossible to use due to its static nature without creating an ACL hell. The more specific permissions set in Active Directory the more difficult it is to maintain. The performance of Active Directory is severely impaired by an overly complex access control policy. For maximum performance, Microsoft recommends a minimal number of Active Directory objects to which specific access control lists are assigned (For more information on this topic refer to Microsoft KB article Q271876). Recent tests have also shown that Active Directory objects grow at approximately 70 bytes per ACE. The increase in database size is probably the most compelling reason one should consider the alternatives (For more information on this topic refer to Microsoft KB article Q197054). Directory and Resource Administrator addresses the issues with the Active Directory's Delegation of Control Wizard by providing granular delegation that is not only easier to maintain but is dynamic by nature. Directory and Resource Administrator delegation model uses the ActiveViews technology, which keeps the Active Directory pure and pollution free. The dynamic ActiveViews technology helps reduce administrative costs involved in maintaining the delegation model on an ongoing basis. It keeps up with the constantly changing environment without any user intervention allowing one to concentrate on other more important tasks. The ActiveViews are like virtual containers, which allow the delegation\security model to spans domains and OUs, to include OUs from multiple domains, other ActiveViews unlike Native tools, which is restricted only to one OU in a domain. The following example illustrates the dynamic security model and its benefits;

> To delegate Bob the ability to reset passwords and update the Description field only for all users in the Sales organization irrespective of where the user object reside. One can use Directory and Resource Administrator to create an ActiveView to include all users in the local group called Sales and assign Bob to the ActiveView. The local group could also include users from NT domains, multiple OUs, Active Directory etc. Once an ActiveView is created to include all users in the local group Sales any time a user is added to this group, Bob will automatically be able to reset the new user account's password and modify the Description field without any intervention on the part of an administrator.

Directory and Resource Administrator uses a 3-tier architecture, which maintain security at the middle tier. This is the standard approach in every major LOB applications such as SAP, Oracle, Seibel, PeopleSoft, Microsoft Great Plains business solutions etc. This eliminates the need to create two accounts for the administrators; one for normal day-to-day functions and the other to carry out their administrative functions to prevent malicious code from spreading through the network with administrator privileges.

Policy Enforcement

This feature allows you to control not only the data that is entered into Active Directory but also the format in which it is entered. This server side policy enforcement feature prevents local administrators and Help-Desk users from entering "garbage" into Active Directory no matter which machine they use. Garbage in is garbage out so it is essential to maintain the integrity of this database. The following example illustrates the benefits of policy enforcement;

> In a company that has project managers one would be amazed on how many ways their titles could be entered into the directory, which would make any kind of reporting useless. The following list shows some of the possible;
>
> Product Manager
> Product Mngr
> Prod Manager
> PM
>
> Some may even misspell or mistype manager and some titles may be completely blank so how would one query the database to search by Title for all product managers in the company. One may have the best reporting tools in their environment but if there is no control over the data entered into the directory then all those tools will report garbage information, which is neither accurate nor dependable.

Directory and Resource Administrator policies can be applied to actions performed by an individual administrator or by all administrators. Following is an example where one may need to selectively apply policies.

> A company with a naming convention policy requires computer accounts to be prefixed with a 3-digit site code. Computer accounts created in the Houston OU should be begin with HOU whereas computers created in the Austin OU should being with AUS. This can be accomplished by selectively applying policies so that when administrators in Houston create a computer account it must being with HOU.

The policy enforcement feature allows one not only to control the data and format of any property in the Active Directory but can also make certain properties mandatory. It ensures that administrators adhere to the policies and standards defined by the company. It also ensures that data in the directory is complete, accurate, valid and moreover reliable and dependable.

Automation

Automating routinely performed tasks reduces administrative burden and improves the efficiency of the administrative staff. The automation feature allows one to specify scripts to perform certain routine tasks, which run before and/or after any operation performed by the administrators. . The following example illustrates the benefits of automation;

> When a user account is created, the process of creating the home directory, setting permissions on the directory and creating an Exchange mailbox can all be automated. In addition to this a post-task trigger can be specified to assign a logon script, modify group memberships and distribution list membership based on which OU or domain the object resides in.

One can also setup a trigger to send an email notification to the Security Administrator when the membership of the Domain Admins group is modified.

Policies and Automation triggers can also be setup to enforce Microsoft's best practices to allow only universal groups to be mail-enabled for Microsoft Exchange 2000 and in plugging security holes, which can occur in Windows 2000 environments. An example of this is exploiting the "Trusted for Delegation" flag on a computer object in Active Directory. As per Microsoft KB article Q283201 it is strongly recommended that caution be exercised when checking this flag since delegation is a very powerful feature and can be misused.

Reporting

The reporting feature significantly improves security by providing an audit trail, which cannot be turned off. It provides detailed reporting on who can do what to whom. This feature lets you report on all administrative functions carried out in your enterprise. There are over 75+ reports available and are presented in an easy to understand format.

Web Console

The Web Console provides a task centric console, which does not require any software to be installed on client machines. It allows administrators to perform their day-to-day tasks from any machine on the network and requires very little or no training at all.

One can avert the disaster now by planning before Active Directory is implemented because failing to plan is planning to fail. If companies deploying Active Directory do not plan now not only will they be compromising the security of the enterprise, but one year down the road they will have to spend a hefty amount of money and resources to clean up the database.

The NetIQ Administration Suite includes the most comprehensive set of administration tools to manage your Windows NT, Active Directory, and Exchange environments. The suite includes Directory and Resource Administrator, Directory Security Administrator, File Security Administrator and Group Policy Administrator (included in the Advanced Edition).

Directory Security Administrator provides the ability to manage the Active Directory security model by providing Resultant Permissions Analysis, ability to search where permissions have been granted to users, groups or machines thus allowing one to reduce the any security risks.

File Security Administrator allows one to manage and report on file security. It provides the ability to delegate the management of files, folders and share. File Security Administrator also allows one to backup and restore NTFS permissions.

Group Policy Administrator, included in the Administration Suite Advanced Edition, simplifies the management of group policies by providing Resultant Set of Policies, reporting, delegation, and the ability to replicate and move GPOs between domains and forests.

Research Links

http://www.netiq.com
http://www.netiq.com/products/dra/default.asp
http://www.netiq.com/products/admin/default.asp
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q271876
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q197054
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q283201