NT Group and User Management Strategies: Part III

BY GUY C. YOST

This month's column concludes this series by exploring the "Policies" option from NT's User Manager main menu. From here, administrators establish trust relationships between domains, configure account and password parameters, assign system "rights" to users, and configure system auditing.

TRUST RELATIONSHIPS

The logic and strategy of using domain trusts were covered in Parts I and II of this series,however, I left the mechanical "how-to" aspect until now.

The first time I wanted to establish a trust relationship between two domains, I assumed that because Server Manager deals with managing NT domain controllers and trusts are between domain controllers, then I would find a "trusts" option in Server Manager. I combed its menu options a dozen times before breaking out the documentation and discovering that trusts are established in User Manager.

From the Policies menu, choose "Trust Relationships" at the bottom. The screen shown in Figure 1 will appear.

Since it takes two to tango, remember that the domain with the user accounts is the "Trusted" domain, and the domain with the resources is the "Trusting" domain. Establishing a trust relationship requires performing explicit actions in each participating domain.

First, from the Trusted domain, click on the bottom "Add" button, and provide the name of the Trusting domain along with that domain's administrator password. Second, from the Trusting domain click on the top "Add" button and provide the name of the Trusted domain along with the Trusted domain's administrator password. Both actions require being logged into their respective domains as administrator or equivalent. This establishes a one-way trust between the domains. The user accounts in the Trusted domain can access the resources in the Trusting domain.

To establish a two-way trust where users in each domain can access resources in the other requires that the process be repeated, however, the roles of each domain must be reversed. When a two-way trust is completed, you would see the same domain listed in both the upper and lower domain lists in Figure 1. A one-way trust would only show the participating domain in either the upper or lower listing, depending on that domain's role.

Removing a trust relationship also requires two steps,one in each domain. The Trusted domain must remove the Trusting domain from its trusting domain list, and the Trusting domain must remove the Trusted domain from its trusted domain list. If a trust is broken, then the entire process must be repeated to re-establish the trust.

Account administrators will likely want to control how users in the domain can use passwords. From the Account option, you will see several options as shown in Figure 2.

It's a good idea to have users change their passwords periodically. You can enforce this by setting passwords to expire after a predefined number of days. Typical expiration is 30 to 45 days. Minimum password age is used to ensure that users keep their new passwords for a defined interval. Otherwise, a user could change his password back to his "old-favorite" immediately after it expires. Having a minimum password length greater than five characters ensures tighter security. By allowing blank passwords doesn't mean that all existing passwords are cleared, it just permits users with no passwords to login. Note that the selections are mutually exclusive. That is, I can't allow some users to login using no password, while those who have a password must conform to a minimum length. Enforcing unique passwords allows NT to remember up to 24 previous user passwords.

Administrators may also want to know about intruders; defined as someone who tried to login with a known user id, but missed the password. In Figure 2, after five incorrect login attempts within 30 minutes the account will be locked until the administrator is notified and unlocks the user's account. Stricter security would lower the number of login attempts or raise the time interval, or both.

The next option forces remote users (connected via RAS) to be logged out of the network when login hours expire. The last option should be left unmarked unless the administrator wants to be involved in changing user's passwords when they expire.

USER RIGHTS

NT defines the term "rights" not as what operations a user can perform on a particular file or directory (permissions), but as what functions or privileged operations can be performed on a server or domain. Under the Policies menu, choose User Rights to display Figure 3.

NT comes with predefined groups that describe what rights are assigned to them. For example, the group Backup Operators possess the right to backup files and directories along with the Administrator and Server Operator. The easiest way to assign User Rights is to simply put users into the predefined groups rather than adding them here. Customization is possible, however, by creating special groups that possess a unique combination of system rights by adding them to the appropriate rights list as

Figure 1: Setting Up Domain Trusts

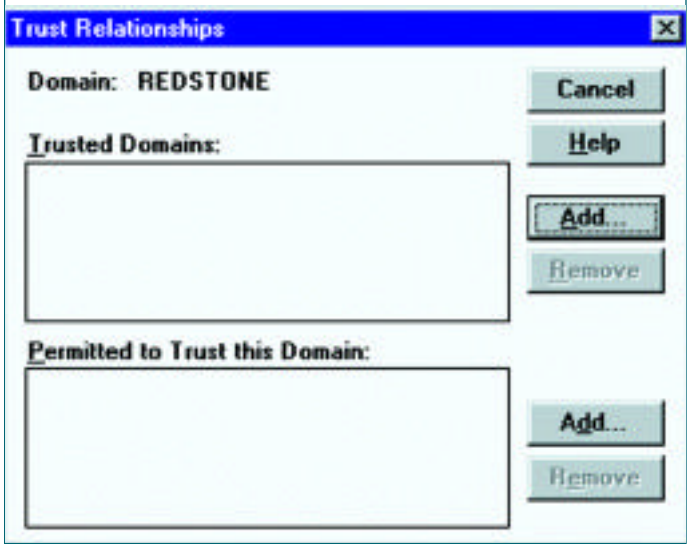
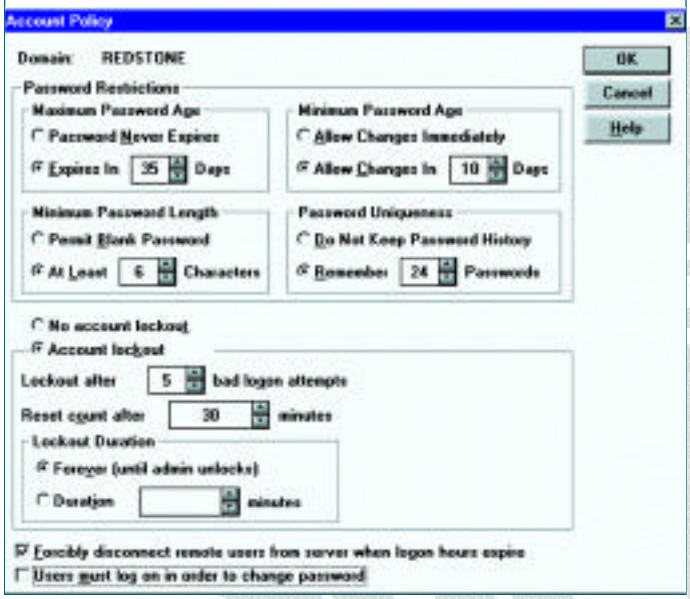


Figure 2: Controlling User Password Parameters



shown in Figure 3. For example, I created a group called Backup and Server Operators and added it to the backup list shown, as well as to the lists where Server Operators are shown. The groups' members would then possess that unique combination of rights.

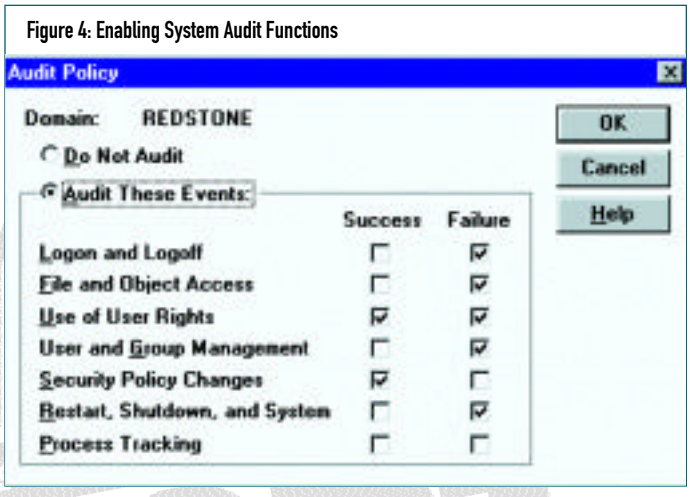
Advanced user rights are normally used by developers, and are not meant to be assigned to users and groups. For example, the rights "Act as part of the Operating System," and "Logon as a Service" are used by third-party NT software utilities and services such as FTP, web and RAS servers.

AUDIT

Certain user activities can be tracked by logging security events. Figure 4 shows the types of events that will be recorded in the shared domain-wide security log file. The audit log contents are examined using the Event Viewer found in the Administrative Tools program group. There are three log file types: System, Application, and Security. Events from configuring this screen will be found in the Security log; a key icon denotes a successful operation, while a failure is shown as a lock.

Figure 3: Assigning User Rights

Figure 4: Enabling System Audit Functions



Be careful how much you choose to audit. Many of the events are truly uninteresting and can consume the limited audit file space quickly. Note that administrators are likely to be most interested in failures of common events (like logging in or out of the domain) and successes of administrative events that would affect system security.

SUMMARY

The degree to which you'll use these features will depend on the level of security required in your network environment. Many administrators choose to only use a portion of these features, but that doesn't mean that they are missing any part of NT's abilities. Whenever possible, keep it simple.

Next month, I'll examine NTFS file and directory permissions and how to protect your network from some sticky NT defaults that could make your system extremely vunerable. As always, thanks for reading. ts

NaSPA member Guy C. Yost is the owner of Redstone Consulting, an IT management consulting firm in New York. He has authored several books on networking for Que Publishing, including Learning NetWare 4.1, and NetWare 4.1 SmartScan, and contributes to Technical Support magazine as an author, columnist and technical editor. Guy also develops and conducts seminars on networking with Windows NT, UNIX, NetWare and Internet/intranet technologies across the United States and Canada. He can be reached at (518) 674-5606 or gyost@logical.net.