NT Group and User Management Strategies

BY GUY C. YOST

Normally this column focuses on the specific use of NT management utilities. However, as I started explaining the various features and menus in NT's User Manager utility, I realized that past columns have always advocated separating education from skill. I found my first pass at writing this month's column leaning toward skill (what buttons to click, menus to pull down, etc.) with little explanation on a topic that really needs to be prefaced with understanding and strategic planning. This month's column will explain this complex topic in detail, and next month I'll break out the screen dumps.

THE GOLDEN RULE

Manage user accounts by putting them into groups, and then manage the groups: That's the fundamental rule for administering any network on any operating system. No matter how small an organization is, create groups. Even if there's only one sales person, create a group called Sales and put the single user in that group; then assign the Sales group access to whatever set of applications are required for the sales person to be productive. The management efforts to accommodate additions or personnel changes to the Sales group will be nominal because of the work completed when the group was established. There is no more initial effort involved in establishing group access control than for the individual. In either case you will need to assign appropriate access rights to applications, printers, data directories, and communication services at least once, so it makes sense to concentrate that effort toward a reusable "umbrella," rather than repeating the process for every user.

Manage user accounts by putting them into groups, and then manage the groups: That's the fundamental rule for administering any network on any operating system.

THE PAINS OF NT ACLS

Group management is essential to good network design. Like UNIX, NT allows group names in the Access Control Lists (ACLs) for network resources. For example, the HP LaserJet printer on Jim's desk has an ACL associated with it, and that list determines which groups and users on the network can access Jim's shared printer, and to what degree. The logical make-up of the ACL looks like Figure 1.

As the owner of the network resource, Jim (or the administrator) can control who can access his printer and what they can do with it. Sales may be limited to just printing, whereas Jim and Jane have the ability to manage the print jobs and other aspects of the printer. To be consistent with the "Golden Rule" at the beginning of this column, groups for managing the printer can be created and placed in the ACL instead of using the User definitions for Jim and Jane. For example, a group called Print Managers can be defined to manage the network printers, and Jane would be in that group. If Jane is on vacation, then the administrator can temporarily put Jane's backup, Ron, in the group.

With NT's ACL-centric design, administrators of "larger" networks (more than 100 users) must be prepared for the labor-intensive nature of managing that environment. That is, for every network resource there will be a corresponding ACL that needs to be maintained as a separate entity. When you think about the number of total network resources in even a small network (consider all applications, directories, printers, and communication devices), the number of ACLs requiring setup and then on-going maintenance can be formidable.

What other approach (besides ACLs) could be used to manage network resources? How about assigning access rights directly to groups of users and domain members, rather than to network resources? You would clearly have fewer total objects to maintain if, for example, you could assign access rights for a list of applications and printers directly to a domain or group name. That's how NetWare and NDS approach user and group management, and hopefully future NT versions will follow suit.

You can't begin to establish user and group management strategies without considering access security. Keep this in mind as you read. Both topics are addressed simultaneously; however, specific information on NT security will be addressed in future columns.

Figure 1: Logical Make up of an ACL

RESOURCE NAME	TYPE	WHO	PERMISSIONS
Jim's LaserJet	Printer	Group Sales	Print Only
		User Jim	Full Control
		User Jane	Manage Documents

Figure 2: Sample Network Resource Matrix

	Domain Admin	Sales	Eng	Mkt	CustSrv	Everyone
Network Resources						
Apps	RXWDPO					
Word	"	RX		RX	RX	
Lotus	"	RX		RX		
ACAD	"		RX			
Paradox	"				RX	
EZ-Mail	"					RX
Data	RXWDPO					
Engineer	"		RXWD			
Marketing	"			RXWD		
Sales	"	RXWD				
CustSrvc	"				RXWD	
Common	"					RXW
Printers						
HP LJ4-Mkt	FULL	Print		Manage	Print	
HPLJ4-Sales	FULL	Manage	Print	Print		
Plotter	FULL		FULL			
Communications						
ShareModem1	FULL	0	x			
ShareFax1	FULL	0		x	x	
TCP/IP gateway		I/O		x		

PLANNING STEPS

Given NT's management characteristics, a game plan should be established before sitting down to User Manager and creating a rash of users and groups. The key is to follow a logical order of creating the network environment.

1. Create (on paper or a spreadsheet) a list of groups and what applications/ network resources they need to access. Make sure all users are placed into one or more groups, depending on their job responsibilities. To accomplish this, I use a matrix structure with all network groups listed across the top (Sales, Marketing, Engineering, Customer Service, Everyone…) and all network resources down the side (Excel, Word, Mail, Project, data directories, printers, communication devices). In the body of the matrix, fill in the cells with what type of access is needed. For example, users will need read-only access to applications, but not all users will need access to the same programs. Rights to some data directories may need to include the ability to write and delete files. In NT, the types of directory and file access are made up of Read, eXecute, Write, Delete, Permissions, and Owner. Details of these permissions will be discussed in a future column. See Figure 2.

2. Create the groups listed in the NRM in User Manager.

3. Create a user template for each group type in User Manager, ensuring that the template is a member of the corresponding group.

4. Create the users for each group using the user template for that group.

The logic behind this order is to first have a written guide-map of the network. The Network Resource Matrix (NRM) serves two purposes. It provides an essential piece of LAN documentation and enables anyone familiar with NT permissions to see, at a glance, what network resources should be granted to which groups. By creating the groups first, you can use the groups when creating the user templates, and thereby save the effort of having to explicitly assign users to groups when the user is created.

TO BE CONTINUED…

Next month, I'll concentrate on how to put these methods to use by exploring specific features and menu options in NT's User Manager utility. At the same time, different kinds of security permissions available in NT will be explained. As always, thanks for reading and for your valuable feedback. *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.