NT Group and User Management Strategies: Part II

BY GUY C. YOST

Last month's column focused on establishing a game plan before setting up NT users and groups. The two main points stressed were to manage users by putting them in groups, then manage the groups; and to create a Network Resource Matrix (NRM) to be used as the network access "master-plan." For reference, Figure 1 shows a partial NRM from last month's column.

Once the NRM is developed, you can use it to guide you through several administrative functions. Just looking at an NRM, you'll know exactly what's needed to create the "ideal" network environment, one that grants user access to enough network resources to be productive, yet is as secure as possible.

CREATE GROUPS

Examine the top row of the NRM in Figure 1. Use NT's User Manager utility to first create the groups, then to create the users through User Manager templates (explained in the next section). User Manager is found in the Administrative tools program group. Creating groups is intuitive and doesn't require a detailed description. Simply choose User from the main menu bar, then New Global Group or New Local Group. Local groups can be used by the current (default) NT domain, whereas Global groups can be used outside of the default domain. The normal group type is Global, unless you have a need for a domain-specific group. Once a group is created, there is little to do in User Manager other than assign members to the group. After users and templates have been created, however, group names are added to the Access Control List (ACL) of the various resources (as indicated by the NRM contents) using File Manager or Explorer.

> **The amount of work required to maintain your NT network is inversely proportional to the amount of time spent planning.**

CREATE USER TEMPLATES

User templates will definitely save time and make network management easier. For each group, create a corresponding user template. For example, in User Manager create a user called "Sales Template" and ensure that the template user is a member of the Sales group. To add the template to groups, simply click on the Groups button shown in Figure 2, highlight the desired group in the "not member of" window, and click the Add button.

You will see that the template user is by default a member of the Domain Users group. A user can belong to several groups, which simply means that the user's security access and permissions are cumulative of all assigned groups. In the group window you will also see a "Set Primary Group" button that is used if running UNIX POSIX or Macintosh applications that use the primary group file and directory access permissions inherent to those operating systems. To set up the template's environment, click on the Profile button, as shown in Figure 2. You will see the screen shown in Figure 3.

The first setting specifies where to look for the user's profile. Profiles define what program groups and desktop functions are presented to the user once logged into the network. Profiles are enabled by default on NT 4 workstations. To ensure that a 95 workstation is configured to use profiles, go to the Passwords icon in the control panel, and select the User Profile tab from the Passwords applet. Simply logging in to the network creates network profiles, and the user's local profile (stored in C:\WINDOWS\PROFILES\<username>, or C:\WINDOWS) is copied to his assigned home directory by default. Users will be able

Figure 1: Partial Network Resource Matrix

	Domain Admin	Sales	Eng	Mkt	CustSrv	Everyone
Apps	RXWDPO					
Word	"	RX		RX	RX	
Lotus	"	RX		RX		
Data	RXWDPO					
Marketing	"			RXWD		
Sales	"	RXWD				
Printers						
HPLJ4-Mkt	FULL			Manage		Print

Figure 2: Configuring User Templates

Figure 3: Setting Up User Environment Paths

to access and update their "roaming" profiles from any computer on the network. The main user settings are stored in a file called NTUser.DAT (for NT workstation users) or User.DAT (for 95 workstations). These files can be renamed to *.MAN, indicating a mandatory profile — one that won't be updated. Mandatory profiles might not be appropriate for everyone, but administrators can use them to present consistent, low maintenance environments for particular users.

Mandatory profiles can also be shared among groups of users. You can specify an alternative directory if you want to store and manage profiles more centrally, as shown in Figure 3. Login to the network using the template user, arrange the desktop to match the needs indicated by the NRM for the group, exit, then rename the template's USER.DAT file to USER.MAN. All users created by the Sales Template will use this centrally referenced profile.

Note that you can also specify a login script (a BAT or CMD file) to further set up a user's environment when they login. Examples of batch file commands would be as follows:

```
NET USE O: \\APPSRV\APPS\OFFICE
NET USE LPT1 \\PRINTSRV\HPLJ5
```

The exact contents of the login batch file will be determined by the group (or user) needs — again referring back to the NRM as the guide. By default, login scripts are expected to be in the domain controller's \WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS directory (shared as NETLOGON).

The user's home directory can be defined as either local (e.g., C:\MYDOCUMENTS) or on a central server. Storing users' files on a server has several important advantages:

◆ centrally accessible data
◆ central back-up and restore
◆ centralized administration and troubleshooting

Note: The NET.EXE command can be used for several functions, and will be featured as the central topic in an upcoming article.

CREATE USERS

Once the templates are configured, the task of creating users is trivial. From User Manager's main screen, simply highlight the template name in the User's section and press F8 to copy the template to a new user name. Simply type in a unique name and password, then click the Add button. You will be prompted to enter information for another user until Cancel is pressed. The new users will inherit all of the template settings, but you can configure individual user settings if desired.

SUMMARY

The amount of work required to maintain your NT network is inversely proportional to the amount of time spent planning. Keep in mind that all of the techniques and methods described in this column series not only apply to new networks, but to established networks as well. In either case, start with creating the NRM and the rest will follow. Next month I'll conclude this series by exploring the Account, User Rights, and Audit options located under the "Policies" option on the main menu. 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.*