CHAPTER 2

Understanding Solaris User Account Management

The corporate data center landscape is changing. While a few years ago mainframe computers and UNIX servers dominated the data center, Windows NT servers are now becoming major players. It is now common to see Windows NT servers and UNIX servers side by side, providing services to the same population of users.

One of your most common tasks as a system administrator is managing user accounts. While the concept of user accounts is shared between Windows NT and UNIX operating systems such as the Solaris operating environment, the implementation differs. Even though you may be comfortable managing user accounts in one environment, you may not be so comfortable in a different environment.

The purpose of this chapter is to provide insight into how user accounts are managed in Solaris software so that you can effectively manage user accounts in both environments. The intent is not to provide a comprehensive text on Solaris system administration techniques, but rather to draw comparisons between Solaris software and Windows NT, highlighting the differences.

Evolution of Network Operating Systems

The concept of a user account has changed over time. With the advent of networked computing, users now access services provided by several computers during the course of a day and not just the computer they initially log on to. The way Solaris software and Windows NT handle network logons differ in some aspects. Since some of these differences are the result of how the two operating environments evolved, it's worthwhile to look back at the evolution of network computing.

Early UNIX Computers

UNIX has its roots as a *multiuser* operating system with users connecting to a UNIX server via ascii terminals. In this environment, users have accounts established on the server they are attached to. The purpose of the account is to grant the user permissions for reading and writing files and executing programs. Since local area networking had not come onto the scene yet, users only required access to the computer they were directly attached to. Therefore, all the user account information was kept on the local server.

With the introduction of TCP/IP networking, accessing data and executing programs on remote computers became possible. However, to access remote systems using the TCP/IP *telnet* (remote login) and *ftp* (remote file copying) services, users were required to have an account on that system. Because having to input an account name and password each time a remote access is made is very inconvenient, Solaris software provided a feature allowing users from trusted systems to log into, run programs on, and copy files to and from a remote system without having to supply a user account name and password each time. However, a user account still needed to be maintained on that remote system, which created administration headaches.

With the introduction of UNIX workstations, which replaced the character-based multiuser systems, remote access to other computers became the norm and not the exception. To facilitate file sharing, which was cumbersome using `ftp`, Sun invented Network File System (NFS) and Network Information Service (NIS). NFS provided transparent file access, while NIS provided a central place to store user account information. Instead of maintaining an account on the local system, the account information was stored on a central server.

Early Personal Computers

Unlike UNIX, which was a multiuser operating system, personal computers (PCs), as the name suggests, were standalone systems. Since there was only one user at a time and networked computers had not evolved, there was no need to maintain user accounts. This situation changed when PCs began to be networked together.

Microsoft's first entre into the network operating system world was Windows for Workgroups (WFWG). Unlike UNIX, which supported `telnet` and `ftp`, WFWG employed LAN Manager file sharing as its main protocol. WFWG supported two modes of file sharing: *share* mode and *user* mode. In share mode, files could be shared so anyone could read or write to them. In user mode, a username and password were required to access shared files. Each computer kept its own list of users and passwords, much like Solaris software did before NIS was created.

Solaris NFS vs. Windows for Workgroups

The difference between how NFS access is controlled in the Solaris operating environment and how file share access is controlled with WFWG has more to do with the file system structure than with the network protocol. WFWG uses the DOS FAT file system which does not have the notion of file ownership or access rights. In contrast, each file or folder accessed via NFS has an owner and access rights that can be set.

Because no access rights are maintained in the file system itself, the only control WFWG has is at the share level. WFWG controlls access rights by maintaining a list of users who can have access to a file share. NFS generally does not maintain a list of who has access rights, passing that responsibility to the underlying file system. Therefore, there is no notion of share level and user level access. In a sense, NFS uses share level, where the file permissions really dictate what can be accessed and by whom.

WFWG networking has the concept of *browsing*, while NFS does not. In WFWG networking, *workgroups* are created for browsing purposes. Only file shares in a computer's workgroup will show up, for example, `net view`. In Solaris software, there is no notion of a workgroup and no browsing, both of which are perceived as an unnecessary use of network bandwidth.

File System Access Rights

Both Windows NT and Solaris software support groups and access control lists (ACLs). User accounts are made members of particular groups when the account is created. A user must be a member of at least one group and can be a member of several. ACLs are a more convenient method than using group permissions for denying access to a particular user or group.

Groups and Access Control Lists

One difference between Solaris software and Windows NT is the use of *world* permissions. Windows NT has the notion of a group called Everyone. By default all users belong to this group. Solaris software does not employ such a group. Instead, Solaris software has the concept of *other* access rights. A directory whose access rights are set to read/write for other in Solaris software has the same effect as setting read/write to the group Everyone in Windows NT.

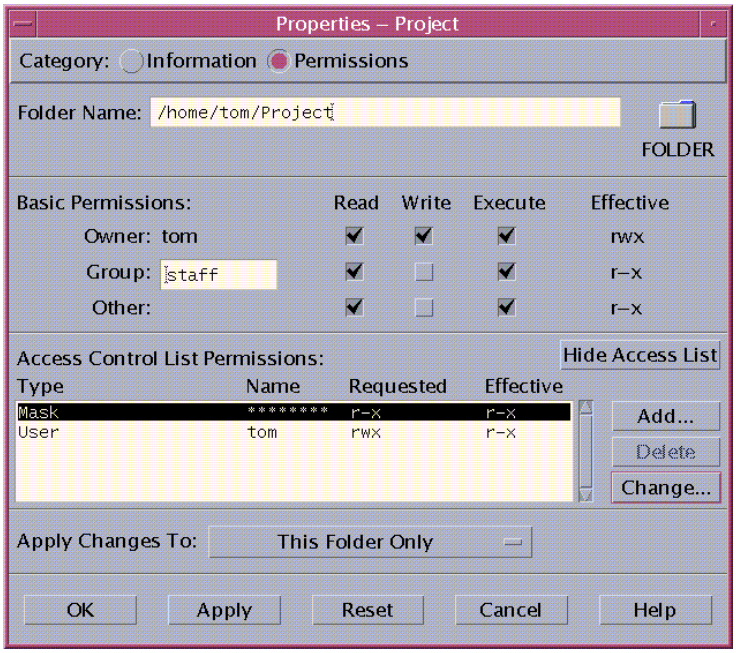

FIGURE 2-1 Solaris File Manager Property Sheet

FIGURE 2-1 shows the Solaris File Manager property sheet for a folder named Project. Solaris software has the notion of setting a *mask*, which dictates what the maximum allowable permissions will be for a given folder and its subfolders. The mask can be changed by the owner of the folder. Using a mask is a convenient method for quickly restricting permission and prevents accidently assigning too high privileges to users or groups.

FIGURE 2-2 shows the Special File Access property sheet found under My Computer. Windows NT provides file permissions similar to those provided by Solaris software. The Delete option in Windows NT is equivalent to setting write permissions on a Solaris directory. A user who does not have directory write privileges in the Solaris operating environment, cannot delete a file in that directory, but can modify one that already exists.

The default behavior in the Solaris operating environment is to allow the owner of a file or folder to change the ownership. This behavior can be changed in Solaris software by setting the RSTCHOWN variable. Solaris software does not have an equivalent to the Take Ownership attribute that is found in Windows NT.

Note – Only file systems formatted as NTFS contain Special File Access properties.

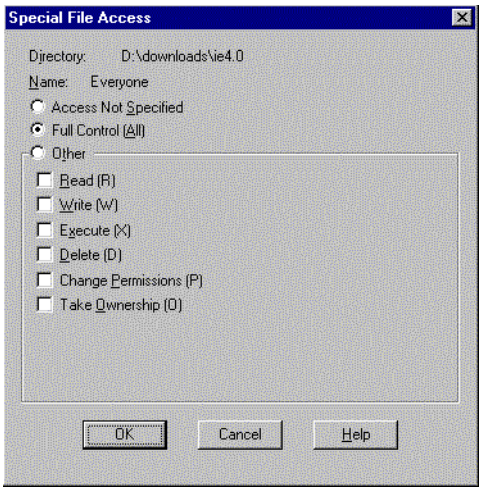

FIGURE 2-2 Special File Access Window

User Account Identification

Both Windows NT and Solaris software associate a number or ID with a user's name. In Solaris software, this numeric identifier is assigned by the system administrator and is called the user ID (UID). The UID is a 16 bit integer assigned to user accounts in the range of 100 - 60000.

Note – Solaris software does not prevent the use of duplicate UIDs, but will issue a warning if an administrator attempts to assign an ID that already exists if the account is created using Admintool. User accounts with the same UID will have the same access rights.

Windows NT creates a security ID (SID) when a new account is created. The SID differs from the Solaris UID in that it is assigned by the system and is not visible to users. A unique SID is created within a Windows NT domain for each user account. If an account with the same name is created in a different NT domain, it will be issued a different SID.

Windows NT also creates a group SID for POSIX compliance. The Group SID specifies a *primary* group, which POSIX requires. The notion of primary group is not widely used in Windows NT.

Note – Since a unique SID is created for each account, once an account is deleted, the SID is lost forever. Even if a new account is created with the same user name as the previously deleted one, a new SID is generated. Therefore, the recreated user account will not have the same access rights as the previous user.

Windows NT and Solaris NIS Domains

As company networks grew and more dependence was placed on shared resources, maintaining user accounts on each computer became increasingly more cumbersome. To ease this management problem, the concept of a *directory* service was created. Instead of maintaining user accounts in a file on a local computer, this information was moved to directory servers that were contacted by the other computers in the network when user account information was required.

Instead of keeping user account information for all the users within a company in one place, separate *name spaces* are created. These name spaces are called Windows NT domains and NIS domains in Solaris software. The servers that maintain these name spaces are called domain controllers in Windows NT and NIS servers in Solaris software.

Similarities

Both directory services maintain user account information on primary and backup servers. In Windows NT terminology, these are called primary domain controllers (PDCs) and backup domain controllers (BDCs). Solaris software refers to them as NIS master servers and NIS slave servers. In both cases, these servers perform the same function. Changes are always made to the PDC or NIS master, then propagated to the BDC or NIS slave. Only one PDC and one NIS master can exist in a domain, while there can be multiple BDCs and slaves. Requests from clients are serviced by either PDC/NIS masters or BDC/NIS slaves.

Differences

In Windows NT, to become a member of an existing domain, the computer name of the client must first be registered on the PDC. Solaris NIS clients do not require that their name be registered with the NIS server before becoming part of a NIS domain.

Windows NT has a notion of *trusted domains*, where a user in one domain can obtain some level of access rights in another domain if it is a trusted domain. Solaris NIS domains are separate entities and do not share any trust relationship. Users who need access rights in another NIS domain must have an account set up there.

Special User Accounts

Both Windows NT and Solaris have a special privileged account that has permission to do anything on the local system. In the Windows NT world this user is called *Administrator*, while in the Solaris world, this user is called *root*. While there are many similarities between these two accounts there are also some differences.

Similarities

- Both are created when the operating system is installed.
- Both are treated as local accounts.
- User rights on the local computer are not automatically transferable to other computers in the network.

Differences

- Login information for root can be kept in NIS, while Administrator is always local.
- Any account with the UID of 0 and GID of 1 has the same access rights as root on a Solaris system. Windows NT allows similar, but not identical access rights to be established for other accounts by allowing membership to Administrator groups.
- The Administrator account cannot be removed, while root can.
- Administrator is included in the group Everyone, while root is treated differently than other. See “Granting Remote File Access Rights to root” on page 12.
- There are certain privileged commands only root can perform unless the `suid` bit is set on the command. See “The Solaris `suid` Bit” on page 12.

Granting Remote File Access Rights to root

Normally, you would expect that if a folder is shared with access rights to Everyone in Windows NT or other in Solaris software that Administrator and root would have those rights. In Solaris software this is not always the case. The default behavior of shared folders in Solaris software is to deny all access rights to root. To override this behavior, the folder must be shared with the `anon=0` or `root=` option.

Note – Solaris software does not have an equivalent of the Domain Administrator group. Placing Administrator users from different Windows NT servers in the Domain Administrator group has the same effect of granting root permissions on remote systems using the `anon=0` and `root=` options.

The Solaris `suid` Bit

Certain functions in Solaris software require that the process performing those functions be run as root. If the process is started via a Solaris command, then that command needs to be invoked by the root user. Sometimes, it's desirable for someone other than root to run the command. In this case, the Set User ID (`suid`) bit is set on the command which gives the command being run the same access rights as its owner, which in this case is root.

An example of a Solaris command which uses the `suid` bit is `ps`, which is used to look at the processes currently running on the local computer.

Guest and nobody Accounts

Windows NT has a built-in account for temporary users called Guest. Solaris software has a somewhat similar user account called nobody. Users who do not have an account in NIS or in the remote system's `/etc/passwd` file, are given the UID of nobody.

User Account Information

Solaris software maintains user account information in a NIS map that gets created from two ascii files: `/etc/passwd` and `/etc/shadow`. The following user account information is stored in this NIS map:

- Username
- Password
- UID
- GID
- Account description
- Home directory
- Login shell

Note – The above information can be either input manually by editing files, or produced automatically by using Solaris tools. If files are edited manually, they can be checked for accuracy by running the `pwck` command.

Username

The rules for creating usernames are somewhat different between Solaris software and Windows NT. The primary things to watch out for are:

- Solaris usernames should be 8 characters or fewer.
- Solaris usernames are case sensitive, hence, “Tom” does not equal “tom.”

Note – Totalnet Advanced Server for Solaris software provides a facility for mapping greater than 8 character Windows NT usernames to 8 character Solaris usernames.

Password

In Solaris software, like Windows NT, passwords can either be assigned by the administrator at the time the account is created, or assigned by the user after the first logon. If the Solaris user changes the password, then it must be at least 6 characters long and have a mixture or alpha and numeric characters.

Password aging can be set using Admintool for `/etc/passwd` accounts and AdminSuite for NIS accounts. Automatic lock out of a user account after a specified number of bad login attempts is not a feature of Solaris software.

Note – Defaults for `/etc/passwd` accounts can be changed by modifying `/etc/default/passwd`.

UID and GID

As discussed earlier, the UID and GID are assigned by the Solaris system administrator. The UID of 0 and GID of 1 are reserved for the Solaris root user account. These fields do not show up in Windows NT because they are generated by the system and kept hidden from users.

Account Description

Account description is a text field for entering the full name and a description of the user. Unlike Windows NT, which has one field called Full Name and another called Description, Solaris software has only a single field.

Home Directory

Solaris software has the concept of a current working directory. When a user logs in, the current working directory is set to the user's *home*. This allows the user to view files and folders that are at or below home. Windows NT has a similar concept where the user's home directory is the default starting point for many file operations.

To allow access to a user's home directory anywhere on the network, home directories are placed on network drives. In Windows NT, this directory is referenced using the Universal Naming Convention (UNC), for example, `\\server_name\folder_name`. Solaris software has a similar method for referencing directories on remote drives called *automounting*. Using the convention `/home/user_name`, the home directory of a particular user can be located by referencing information kept in NIS maps.

Solaris software also makes use of home directories to store login scripts and user profiles. More information on user profiles is provided in the next section.

Note – If a non-existent home directory is specified, or if the user does not have appropriate access rights to it, the users's home is set to "/", which is the top level directory on a Solaris system.

Login Shell

As mentioned earlier, UNIX originated as a character based multiuser operating system. A command line interface, or *shell*, is immediately presented when a user logs in. This is similar to early versions of Windows where a DOS *shell* would first be presented to the user before the Windows GUI was invoked.

As UNIX grew in popularity, many enhancements were made to the original shell. These enhancements came from different sources and resulted in a choice of shells. Solaris software includes the three most popular shells:

- sh—the original Bourne shell
- csh—C-shell, developed as part of BSD UNIX
- ksh—Korn shell, developed at ATT

There is much reference material available on these shells, so their differences and benefits will not be discussed here. One important feature, however, is the ability to specify a start up script when the shell is first started. These start up scripts appear similar to the `autoexec.bat` file in DOS, but are actually more akin to user profiles in Windows NT.

Note – Although this field is typically used for a login shell, a program or script can be specified instead. For example, a user account called halt can be created which simply executes the Solaris `halt` command, then exits.

User Profiles

Solaris software supports start up scripts to establish a user's environment as does Windows NT. Solaris software does this by placing a startup file, `.login`, `.profiles`, `.cshrc` in the user's home directory. These files contain scripts and environment variable settings.

Both Solaris software and Windows NT provide default user profiles. FIGURE 2-3 shows a default user desktop environment in Windows NT. FIGURE 2-4 shows a default user desktop environment in Solaris software.

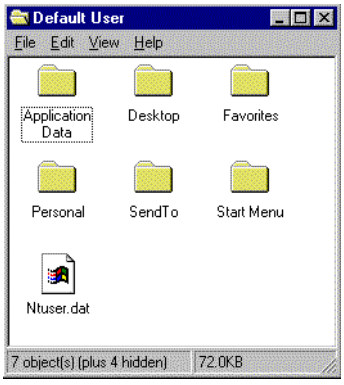

FIGURE 2-3 Windows NT Desktop Environment

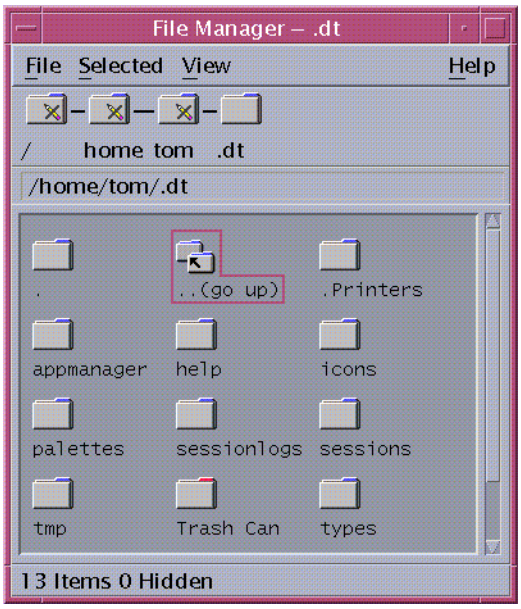

FIGURE 2-4 Solaris Desktop Environment

One major difference between creating user profiles in Solaris software and Windows NT is that Windows NT supports system wide (or NT Domain wide) user profiles. Solaris software always looks in the user's home directory for login scripts. However, system wide login scripts can be created in Solaris software by invoking a common script from the login script in a user's home directory.

Sample Solaris login scripts can be found in `/etc/skel`. These scripts can be modified and copied to the user's home directory as `.profile`, `.login`, and `.cshrc`. Accounts created with Admintool or AdminSuite will have these scripts automatically copied if desired.

Login Process

The process of logging into a Windows NT computer is similar to logging into a Solaris computer. Similar steps are performed, although the underlying system functions are different. The following steps describe the login process at a high level.

1. User types *username* and password
2. The computer checks to see if the user name exists in the directory service and, if so, verifies the password.
3. A local shell is started that reads and executes specified start up scripts.
4. The desktop environment is started.

Solaris Login Process

FIGURE 2-5 shows the Solaris user login process.

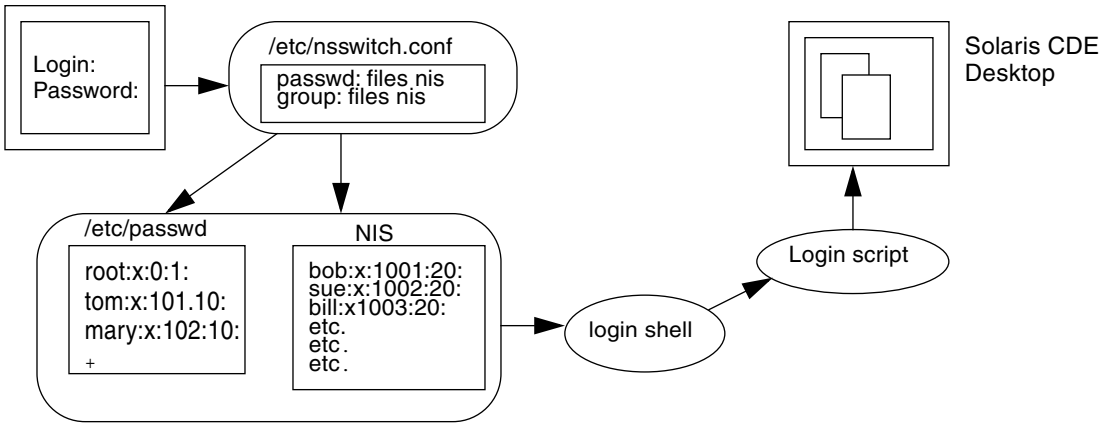

FIGURE 2-5 Solaris User Login Process

Solaris Name Service Switch

One of the unique features of Solaris software is the ability to specify where to look for a user's account information. This allows local accounts in `/etc/passwd` to be created, but at the same time use NIS to find non-local account information. The file `/etc/nsswitch.conf` specifies a search path for locating the user's account information. The default behavior is to first check to see if the user name matches one in `/etc/passwd` and, if so, use that information. If the user name is not in `/etc/passwd`, then NIS is checked to see if it contains that name.

Windows NT Login Process

FIGURE 2-6 shows the Windows NT login process.

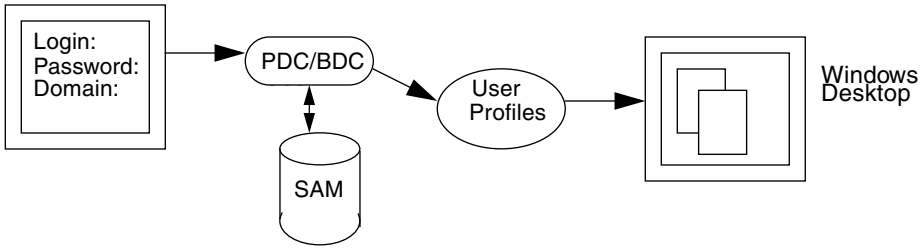

FIGURE 2-6 Windows NT Login Process

Two differences between the Solaris and Windows NT login process should be noted:

- If trusted domains are implemented, then the user will have a choice of Windows NT domains to verify the login
- If a Windows computer belongs to a Windows NT domain, then no accounts on the local computer exists. The PDC/BDC is always consulted in this case. The exception is when Windows NT is deployed as a member server, which can contain local accounts.

Note – If a Solaris user account in `/etc/passwd` has the same UID as an account in NIS, the user logging in using the `/etc/passwd` account will have the same permissions as the NIS account. Therefore, it is advisable to restrict the use of local root accounts so `/etc/passwd` accounts can only be created by system administrators.

User Account Management

Historically, Solaris system administrators have preferred to use command line tools for user account management. However, GUI based tools similar to tools in Windows NT, like Admintool, are available for Solaris software.

Solaris User Account Management

This section only describes the Solaris GUI based tools for adding users and groups and contrasts them with Windows NT tools.

Note – Admintool must be run as root or someone in the `sys` group to add or delete users or modify user account information. Like User Manager for Domains in Windows NT, other users can view the information, but cannot modify anything.

Adding Users

FIGURE 2-7 shows the Add User property sheet, invoked by using the Edit➤Add User property sheet found in Admintool.

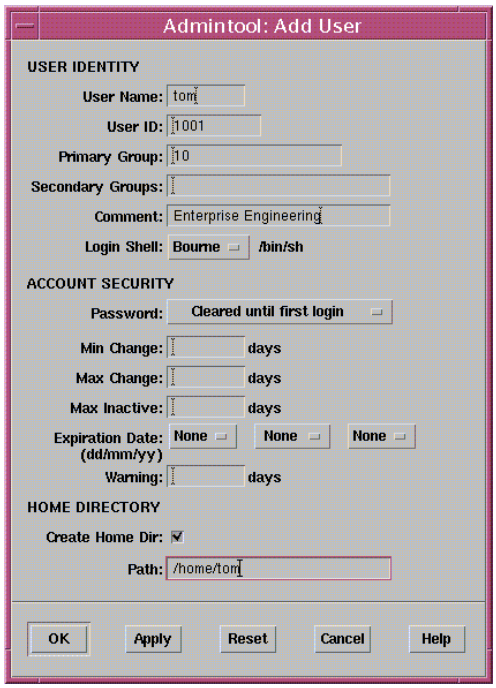

FIGURE 2-7 Solaris Add User Property Sheet

Following are a few of Admintool's characteristics that you should be aware of:

- User ID—Admintool will automatically assign the next highest unused ID.
- Groups can be entered as a name or as a GID.
- Every user must belong to a primary group.
- Secondary groups are optional.
- The `/home/username` nomenclature refers to an NFS file system. The directory that `/home` is mapped to could reside on a system other than the one Admintool is being run from. If it is, the root user running Admintool must have write access rights on that directory.

FIGURE 2-8 shows the Edit➤Add Group screen in Admintool.

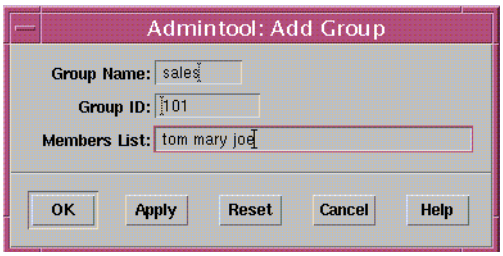

FIGURE 2-8 Solaris Add Group Property Sheet

Unlike Windows NT, Solaris software requires that a unique GID be assigned to each group. The Members List is primarily used to create secondary group membership for users. Members that have the group listed as its primary group will not automatically appear in the Member List.

Windows NT User Account Management

The tools used to add or delete users and modify user account information in Windows NT is User Manager for Domains. Like Admintool in Solaris software, this tool does not need to be run on the same computer that contains the actual account information, that is, the PDC.

FIGURE 2-9 shows the User Properties screen of User Manager for Domains.

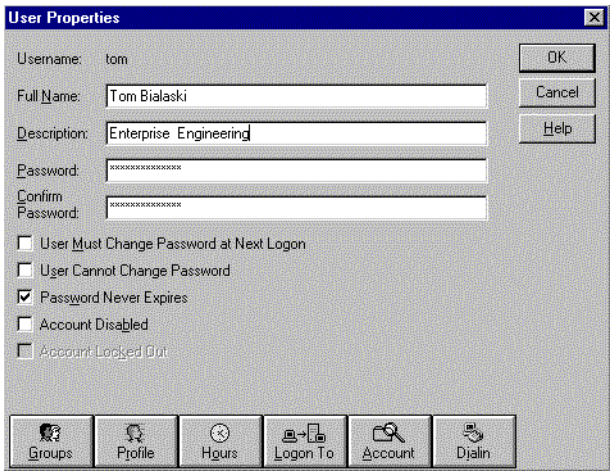

FIGURE 2-9 Windows NT User Property Sheet

The user account information on the main screen is similar to the user account information found in Solaris software. Tools for specifying the hours that a particular user can log in, the systems the user can access, and whether a dial-in login is permitted, are not part of Admintool.

FIGURE 2-10 shows the New Global Group screen which is invoked from the Groups button.

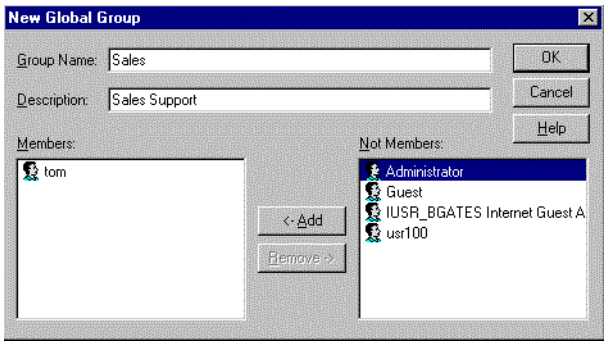

FIGURE 2-10 Windows NT New Global Group Property Sheet

Groups in Windows NT can be either Global or Local. Solaris software does not have the notion of Local groups, which are primarily used with Domain Trusts in Windows NT.