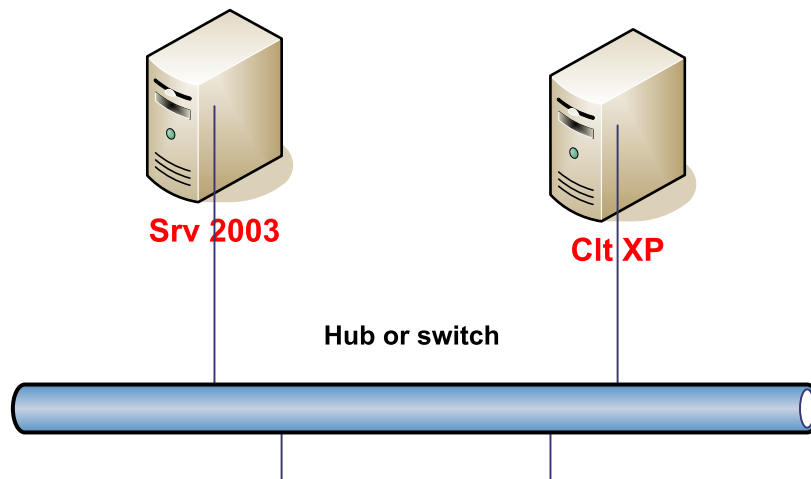


NON ENCADRE

TP 6 : Windows XP & 2003
Managing Users, Computers, and Groups

The professor will indicate the objectives concerning this practical working session.
Each group of four pupils will use a windows 2003 server and XP.



Follow the indications provided in this document and answer the test located at the end.

In the second part of your training Lab :

- Activate and test the windows 2003 services (Dhcp and Ftp). In this case, use an analyzer to observe flows associated with these services.
- If you have enough time, develop a script to manage the users' accounts.

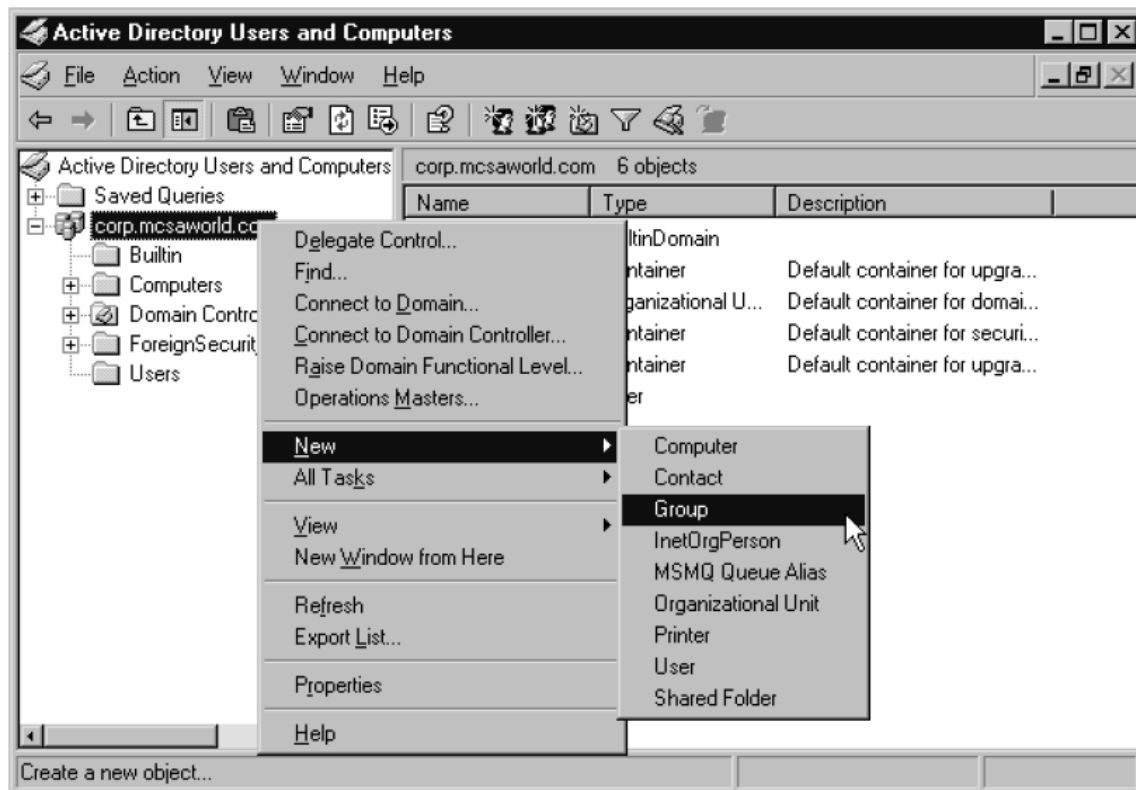
Managing Users, Computers, and Groups

Creating groups with active directory	3
Adding members to group	4
Removing members from groups	7
Changing group scope	10
Deleting groups	12
Modifying group properties	13
Finding groups in which a particular user is a member	15
Determining the groups a user is a member of	15
Assigning user rights and permissions to a group	16
Applying user rights to a group	17
Assigning ntfs permissions to a group	18
Creating and managing user accounts	20
Creating a new user account with ad users and computers	21
Resetting the user account password	23
Resetting user passwords with ad users and computers	23
Copying a user account	24
Copying user accounts from ad users and computers	24
Disabling or enabling a user account	25
Configuring user account properties	25
The general tab	25
The address tab	26
The account tab	27
Configuring user logon time and computer restrictions	28
The profile tab	30
Deleting user accounts	31
Deleting users from ad users and computers	31
Creating and managing computer accounts	32
Creating computer accounts from ad users and computers	32
Creating computer accounts by joining to the domain	34
Joining a computer to the domain	34
Frequently asked	36
Test	37
Extended command line functionality	40

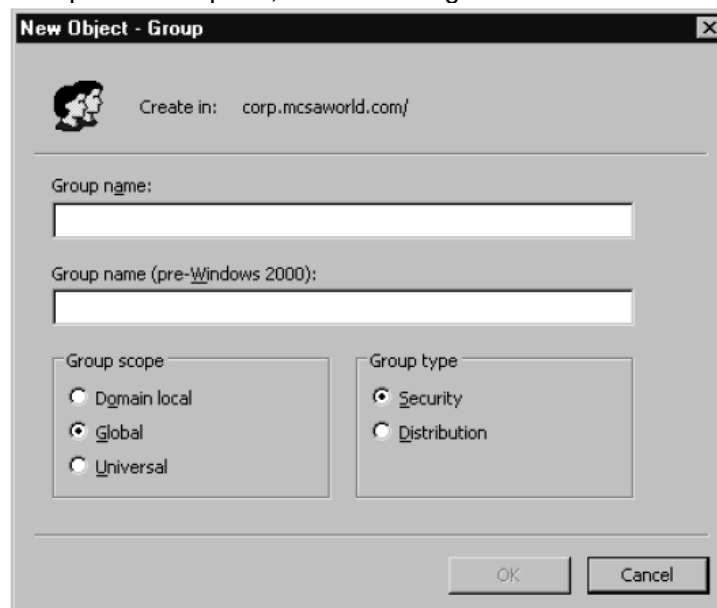
CREATING GROUPS WITH ACTIVE DIRECTORY ¹

USERS AND COMPUTERS

1. Open the **Active Directory Users and Computers** console.
2. Expand the console tree until you locate the node in which you want to create the new group.
3. Right-click on the node and select **New | Group** from the context menu, as seen in Figure.



4. The New Object – Group window opens, as seen in Figure.



¹ **ACTIVE DIRECTORY = AD**

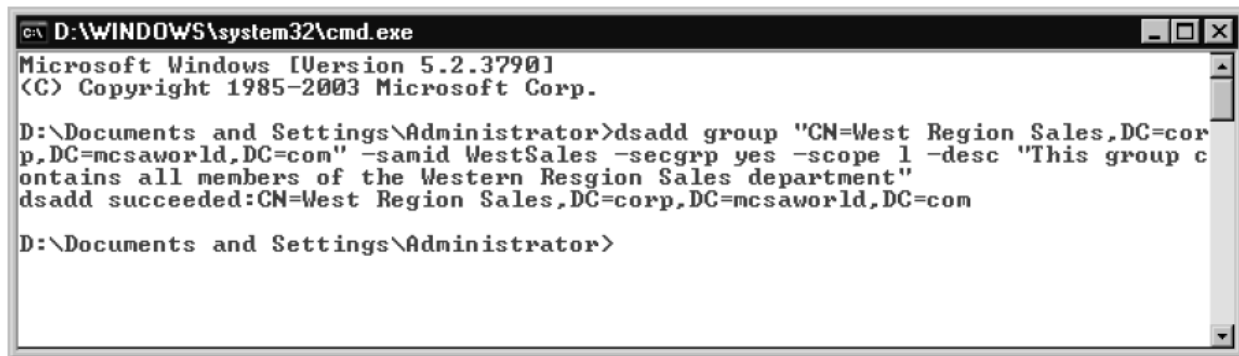
5. Enter the **Group name**. By default, the pre-Windows 2000 Group name is the same; however, you can change it as required to make it compatible with Network Basic Input/Output System (NetBIOS) naming requirements.

6. Select the **Group scope** and **Group type** as required. Click **OK** to create the new group.

New groups can also be created from the command line using the *dsadd* command. The syntax required to create a new group is as follows:

```
dsadd group GroupDN [-secgrp {yes | no}] [-scope {l | g | u}] [-samid SAMName] [- desc Description]
```

Creating a New Group from the Command-Line



```
C:\ D:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

D:\Documents and Settings\Administrator>dsadd group "CN=West Region Sales,DC=corp,DC=mcsaworld,DC=com" -samid WestSales -secgrp yes -scope l -desc "This group contains all members of the Western Region Sales department"
dsadd succeeded:CN=West Region Sales,DC=corp,DC=mcsaworld,DC=com

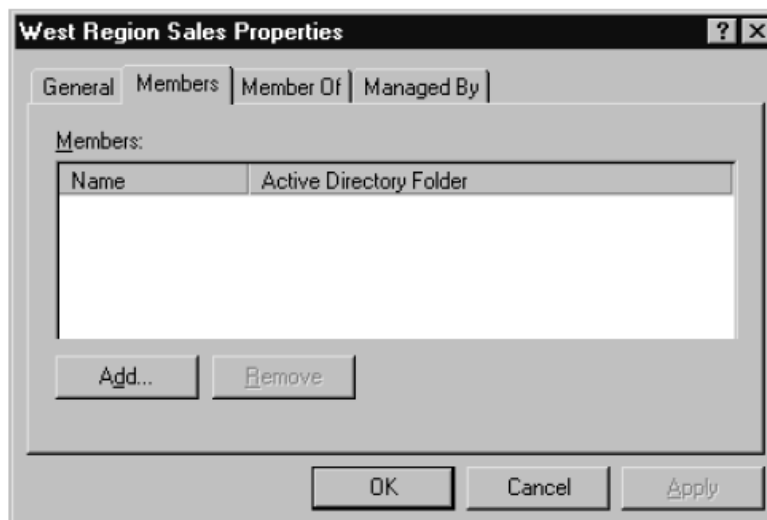
D:\Documents and Settings\Administrator>
```

Adding Members to Group

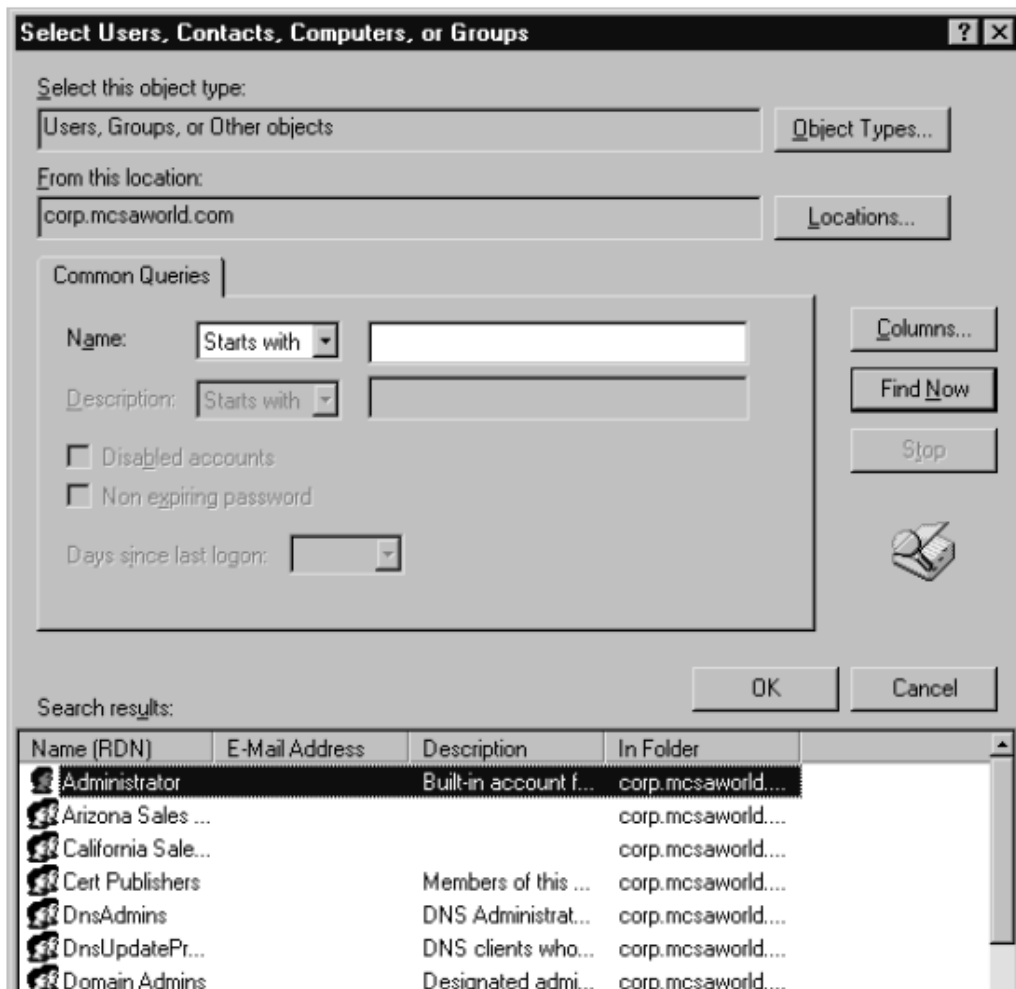
Once a group is created, members are added to it. It is important to remember that group members can be user accounts, computer accounts, or other groups as allowed.

ADDING GROUP MEMBERS WITH AD USERS AND COMPUTERS

1. Open the **Active Directory Users and Computers** console.
2. Expand the console tree until you locate the group to have members added.
3. Double-click on the group to open its Properties dialog box.
4. Switch to the **Members** tab, as seen in Figure.



5. Click the **Add** button to open the Select Users, Contacts, Computers or Groups dialog box. To search for users, click the **Advanced** button. Click **Find Now** to search for appropriate members, as seen in Figure.

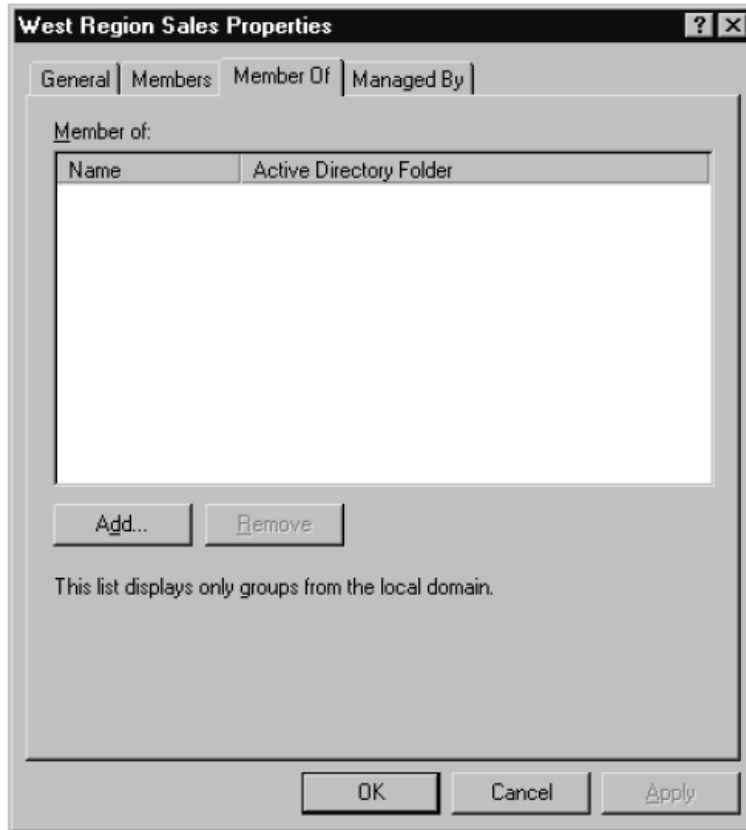


6. To add an account or group, double-click it. To add multiple accounts or groups, click on them one at a time while pressing the **Ctrl** key. Remember that you must abide by the rules for nested groups outlined in the "Group Scopes" section earlier in this chapter. After making your selections, click the **OK** button.

7. After the Select Users, Contacts, Computers or Groups dialog box collapses, click **OK** to confirm and add the selected accounts and groups.

8. Click **OK** or **Apply** to accept the membership change.

9. You can also make this group a member of another group by switching to the **Member Of** tab. The process is the same as the rules for adding nesting groups as outlined in the "Group Scopes" section.



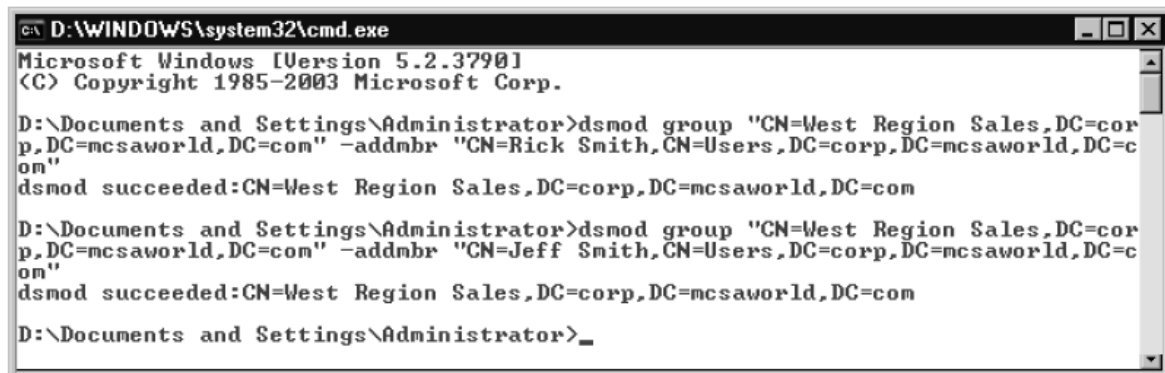
Members can also be added to an existing group from the command-line using the *dsmod* command. The syntax required to add a member to a group is as follows:

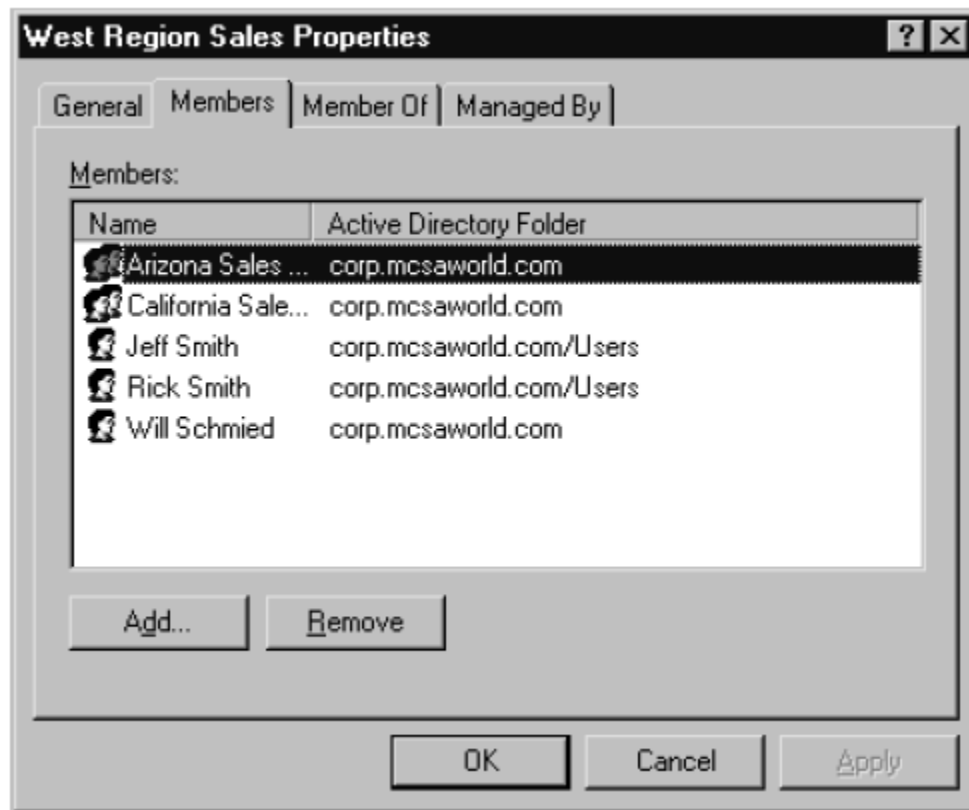
```
dsmod group GroupDN -addmbr MemberDN
```

The function of the switches is self-explanatory, as they represent the distinguished name of the group to add the member to and the distinguished name of the member to be added. Appendix A contains a complete listing of the *dsmod* command and its switches.

To add two user accounts to the West Region Sales group using the following commands:

```
dsmod group "CN=West Region Sales,DC=corp,DC=mcsaworld,DC=com" -addmbr  
"CN=Rick Smith,CN=Users,DC=corp,DC=mcsaworld,DC=com"  
dsmod group "CN=West Region Sales,DC=corp,DC=mcsaworld,DC=com" -addmbr  
"CN=Jeff Smith,CN=Users,DC=corp,DC=mcsaworld,DC=com"
```





Removing Members from Groups

The process for removing a member from a group using the Active Directory Users and Computer console is simple: highlight the member or members to be removed on the **Group Members** tab, seen previously in Figure 1.12, and click the **Remove** button. You will be prompted to confirm your actions before they are carried out.

To remove group members from the command line, use the *dsmod* command. This time, however, the command being issued would look like:

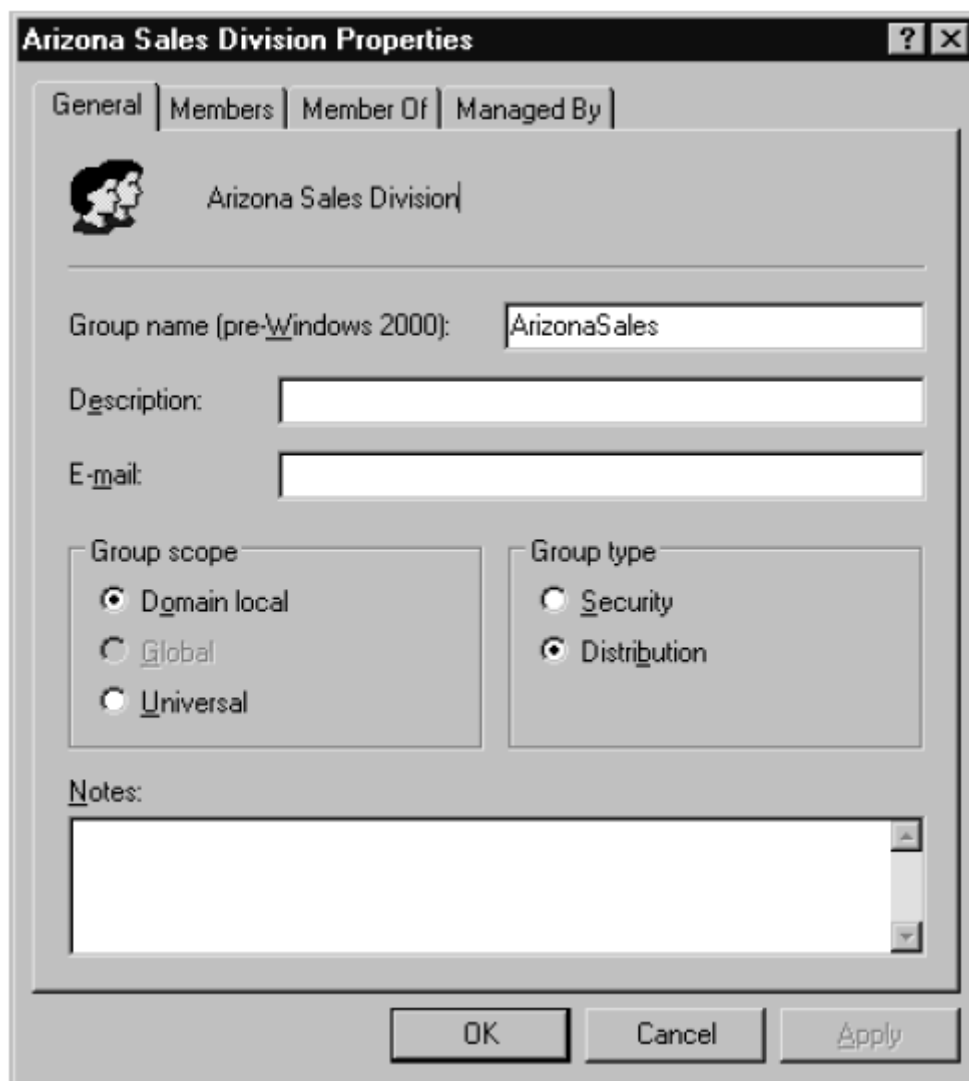
```
dsmod group "CN=West Region Sales,DC=corp,DC=mcsaworld,DC=com" -rmmbr "CN=Jeff Smith,CN=Users,DC=lab1,DC=corp,DC=mcsaworld,DC=com"
```

Converting Group Type

If the domain functional level is Windows 2000 native or higher, security groups can be converted to distribution groups at will, and vice versa. Recall that distribution groups do not have DACL entries and can only be used for e-mail distribution. Security groups can be used for e-mail distribution as well, and can also be used to effectively manage user rights, assignments, and permissions.

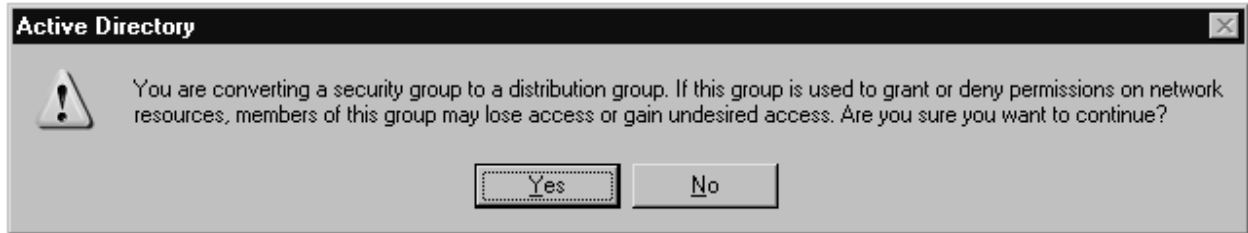
CONVERTING GROUP TYPE FROM AD USERS AND COMPUTERS

1. Open the **Active Directory Users and Computers** console.
2. Expand the console tree until you locate the group whose type you wish to convert.
3. Double-click on the group to open its **Properties** dialog box.
4. On the **General** tab, seen in Figure 1.15, you will be able to change the group type.



5. For conversions from Distribution to Security, you simply make the change and click **OK** or **Apply**.

6. For conversion from Security to Distribution, make the change and click **OK** or **confirm**. You will be warned, as seen in the warning dialog of Figure 1.16, that users may gain or lose access to resources in an unwanted way. This is due to the fact that you are removing the DACLs from the group by converting it to a distribution group.



7. If you want to make the conversion to a distribution group, click **Yes**.

About DACLs

A DACL is an internal listing that is attached to files, folders, and other directory services objects on volumes that are formatted with the NTFS file system. DACLs are configured by administrators and used to specify which users and/or groups are allowed to perform different actions on the file, folder, or object in question. The implementation of a DACL varies from files and folders to other objects due to the specific requirements of other objects. For example, files and folders have the Read access permission, but printers do not.

Each DACL is made up of Access Control Entries (ACEs). Each ACE specifies the security identifier (SID) of the security principal (user or group) that it applies to as well as the level of access to the file, folder, or object that is permitted for that specific security principal.

Group type conversions can also be performed from the command-line command. The syntax required to perform the conversion is as follows:

```
dsmod group GroupDN [-secgrp {yes | no}]
```

Again, the function of the switches are self-explanatory as they represent distinguished name of the group to be converted and the type of group conversion. Appendix A contains a complete listing of the *dsmod* command and its switches.

Examples demonstrates using the *dsmod* command twice, first to convert distribution group into a security group and then back into a distribution group using following commands:

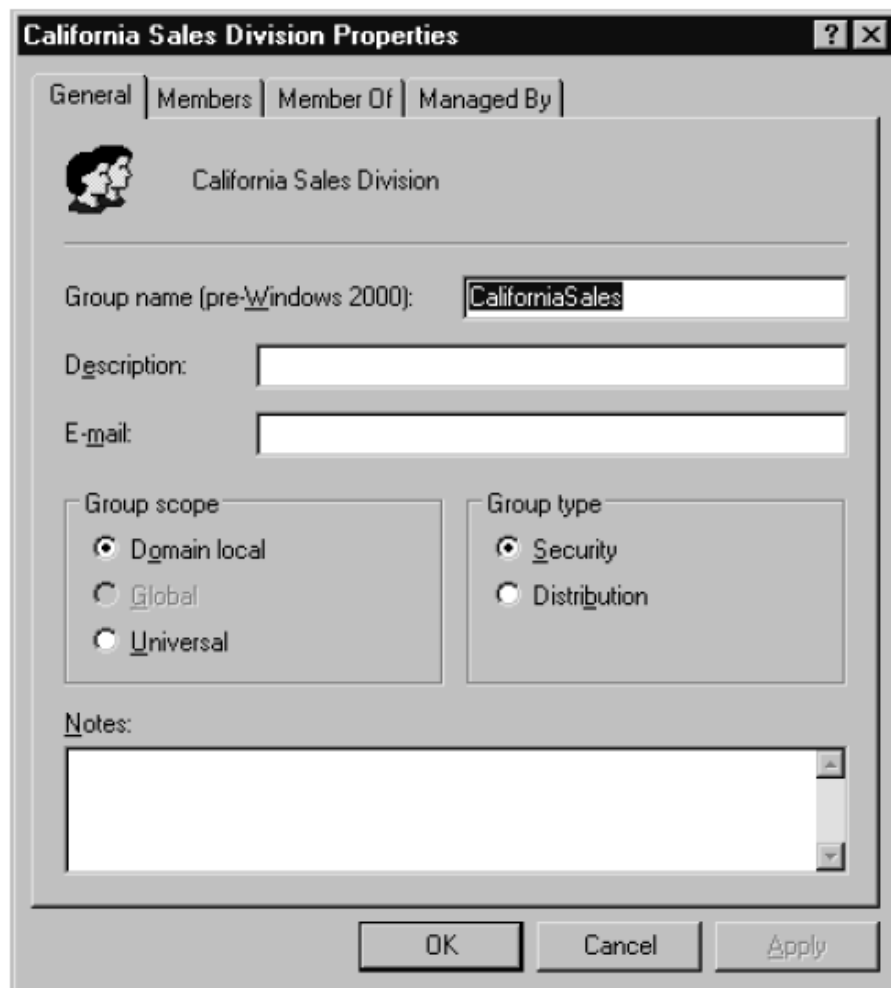
```
dsmod group "CN=Arizona Sales Division,DC=corp,DC=mcsaworld,DC=com"  
dsmod group "CN=Arizona Sales Division,DC=corp,DC=mcsaworld,DC=com"
```

Changing Group Scope

Just as a network administrator might want to convert the group type, they may also need to change the group scope over time. If the domain functional level is Windows 2000 native or higher, they will be able to use Universal groups. A network administrator can change the scope of a group from the Active Directory Users and Computers console by performing the steps outlined below.

CHANGING THE GROUP SCOPE FROM ACTIVE DIRECTORY USERS AND COMPUTERS

1. Open the **Active Directory Users and Computers** console.
2. Expand the console tree until you locate the group whose scope you wish to change.
3. Double-click on the group to open its Properties dialog box.
4. On the **General** tab, as seen in Figure 1.18, you can change the group scope.



5. Change the group scope as desired and click **OK** or **Apply** to accept the changes.

Group scope changes can also be performed from the command line using the *dsmod* command. The syntax required to make scope changes is as follows:

```
dsmod group GroupDN [-scope {l | g | u}]
```

The function of the switches are self-explanatory, as they represent the distinguished name of the group to be converted and the type of scope to change the group to.

Examples using the *dsmod* command three times: first to (unsuccessfully) change a Domain Local group into Global group, second to (successfully) change this same Domain Local group into a Universal group, and lastly to (successfully) change the Universal group into a Global group using the following

commands:

```
dsmod group "CN=California Sales Division,DC=corp,DC=mcsaworld,DC=com" -scope g
dsmod group "CN=California Sales Division,DC=corp,DC=mcsaworld,DC=com" -scope u
dsmod group "CN=California Sales Division,DC=corp,DC=mcsaworld,DC=com" -scope g
```

Deleting Groups

A group can easily be deleted from within the Active Directory Users and Computers console. Note that deleting a group does not cause any members of the group to be deleted from Active Directory—only to be removed from that group and lose any rights and permissions that may have been applied to them if the group is a security group. If the group is a distribution group, e-mails will no longer be able to be sent to the group e-mail address.

DELETING GROUPS FROM ACTIVE DIRECTORY USERS AND COMPUTERS

1. Open the **Active Directory Users and Computers** console.
2. Expand the console tree until you locate the group to be deleted.
3. Right-click on the group and select **Delete** from the context menu.
4. When prompted if you want to delete the group, click **Yes**.

A group can also be deleted from the command-line using the *dsrm* command. The syntax required to delete a group is as follows: **dsrm GroupDN**

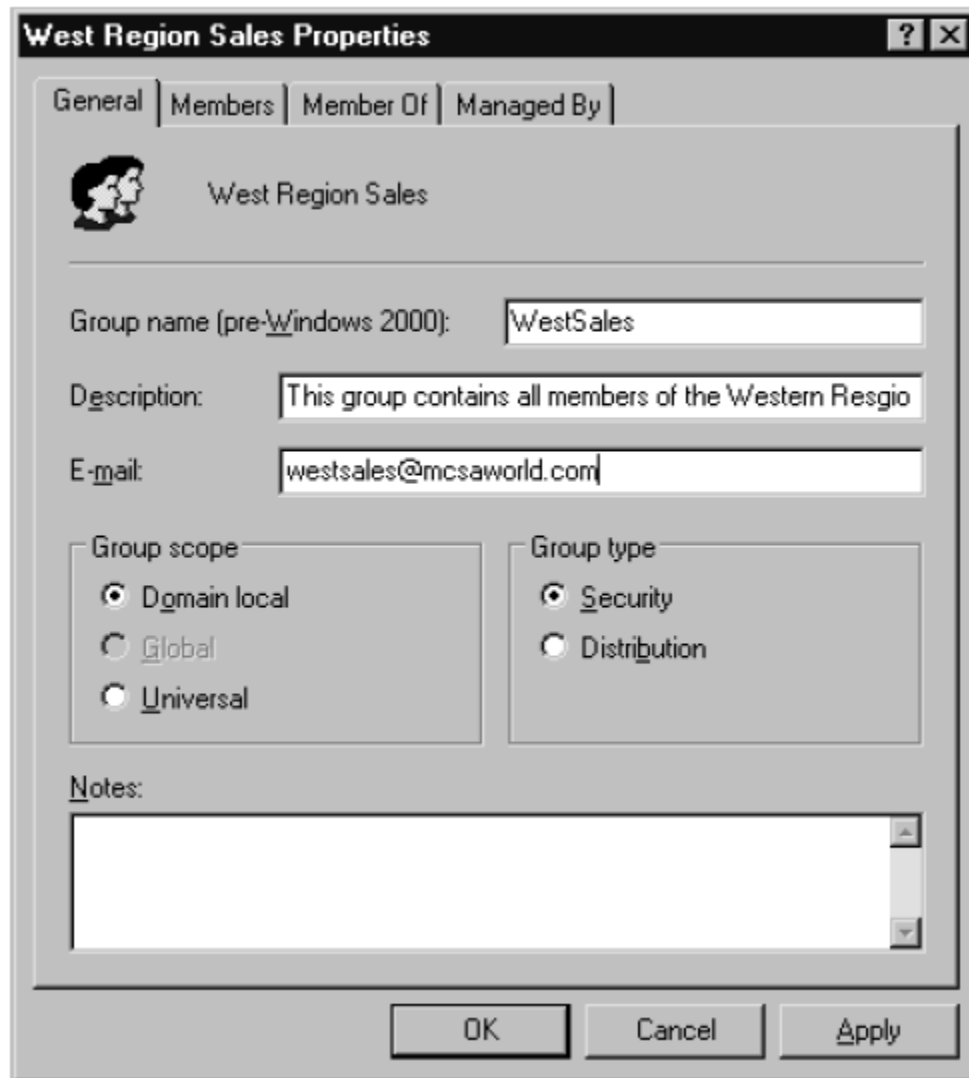
Example using the *dsrm* command to remove the Washington Sales Division group using the following command: **dsrm "CN=Washington Sales Division,DC=corp,DC=mcsaworld,DC=com"**

Modifying Group Properties

After a group is created, the properties may need to be changed. Most commonly, these changes include supplying an e-mail address for the group and denoting someone as being the person responsible for the group.

MODIFYING GROUP PROPERTIES

1. Open the **Active Directory Users and Computers** console.
2. Expand the console tree until you locate the group to have its scope changed.
3. Double-click on the group to open its **Properties** dialog box.
4. On the **General** tab, you can enter an e-mail address to be used to distribute e-mail to all mailbox-enabled members of the group.



5. If you want to list a user as being responsible for the group, switch to the **Managed By** tab. Go through the process to locate and add a user as demonstrated earlier. You will see the pertinent details, as seen in Figure, after confirming the responsible user.

West Region Sales Properties [?] [X]

General | Members | Member Of | Managed By

Name: corp.mcsaworld.com/Will Schmied
[Change...] [Properties] [Clear]
☐ Manager can update membership list

Office:
Street: 325 My Street

City: Any Town
State/province: AZ
Country/region: United States

Telephone number: 480-555-0123
Fax number: 480-555-3456

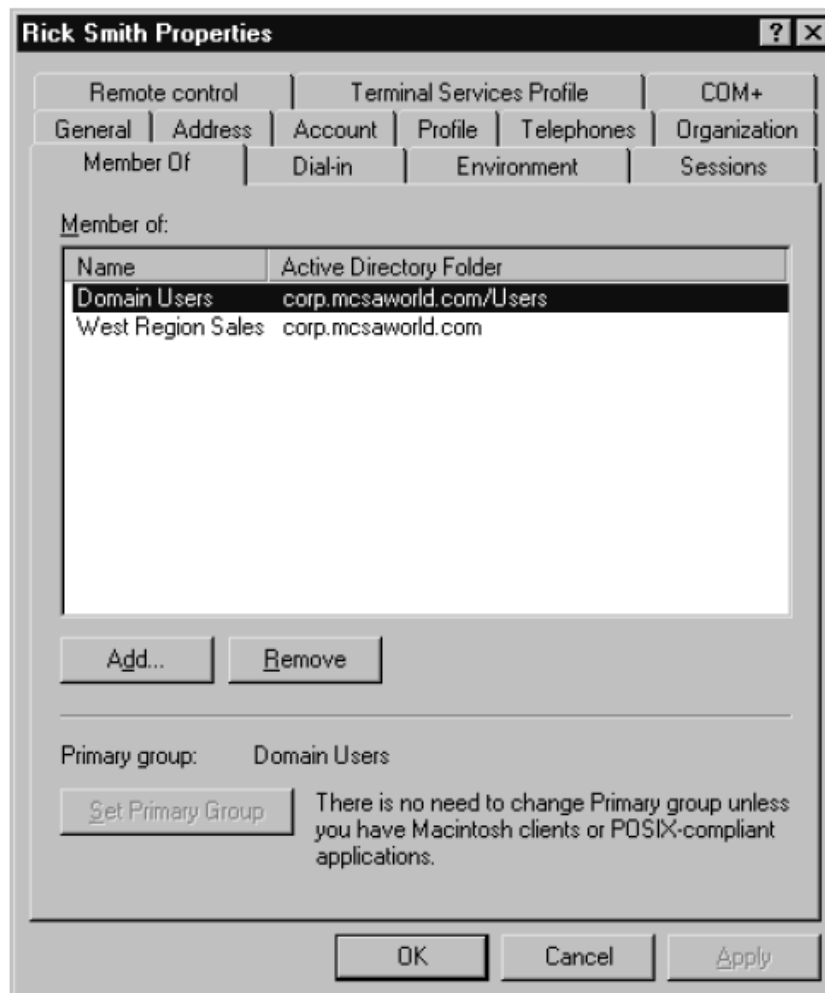
[OK] [Cancel] [Apply]

Finding Groups in Which a Particular User is a Member

The ability to determine which groups a user is a member of can be helpful in many situations, including troubleshooting permissions and user rights assignments. To determine which groups a user is member of (this also applies for computers) from the Active Directory Users and Computers console, perform the steps below.

DETERMING THE GROUPS A USER IS A MEMBER OF

1. Open the **Active Directory Users and Computers** console.
2. Expand the console tree until you locate the user in question.
3. Double-click the user to open the **Properties** dialog box.
4. Switch to the **Member Of** tab, to quickly determine what groups the user is a member of.



To determine what groups a user is a member of from the command-line, use the `dsget` command. The syntax required is as follows: **`dsget user UserDN -memberof`**

Example: `dsget user "CN=Rick Smith,CN=Users,DC=corp,DC=mcsaworld,DC=com" -memberof`

Assigning User Rights and Permissions to a Group

After learning about groups in an effort to make administration of a network easier and more exact, it is only natural that we conclude the discussion of groups with a brief examination of how user rights and permissions assigned to them.

Assigning user rights to a group can be done in several places, each at a different within the overall Active Directory domain hierarchy. The following list contains locations and ways that user rights can be assigned to a group:

Default Domain Controller Security Settings Console Located Administrative Tools folder, this console can be used to configure user assignments for all domain controllers. Domain controllers are located Domain Controllers container in Active Directory Users and Computers.

Default Domain Security Settings Console Located in the Administrative Tools folder, this console can be used to configure user rights that will to the domain as a whole.

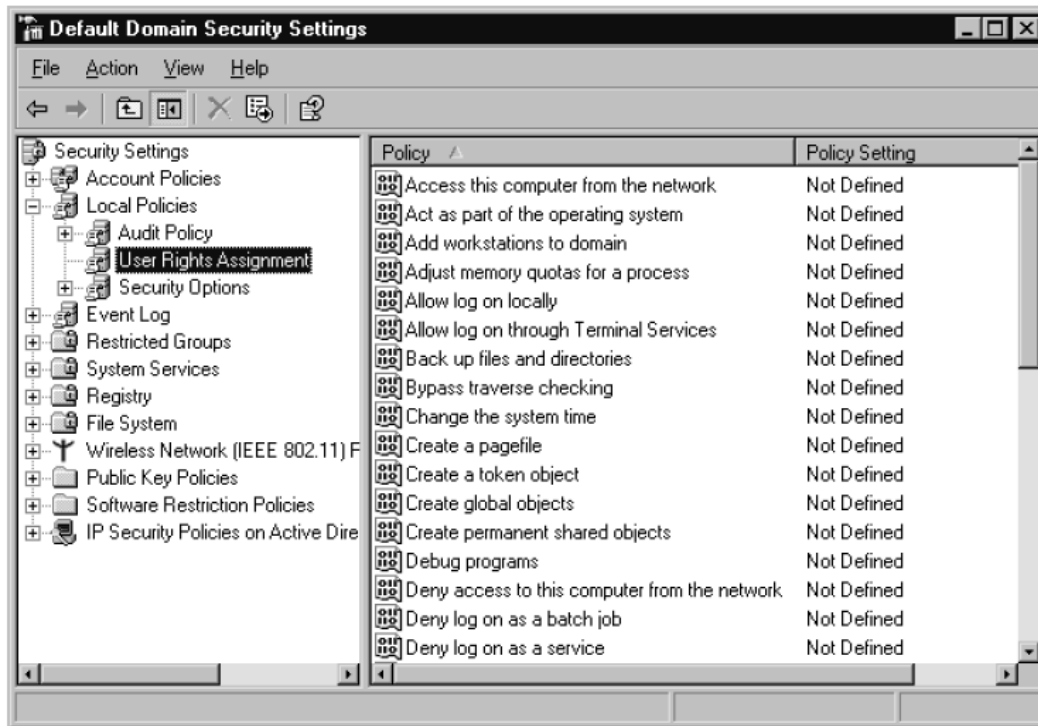
Local Security Policy Console Located in the Administrative Tools console can be used to configure user rights that will be applied only computer.

Group Policy Objects (GPOs) GPOs can be applied at various Active Directory, such as the domain level or to a specific Organizational Within each GPO, user rights can be assigned that will affect all objects has been applied to.

Security Templates Security Templates can be used to quickly and apply security settings to all objects they have been applied to. Security can be applied directly to a local computer or imported into a GPO application to all objects the GPO is applied to. Security.

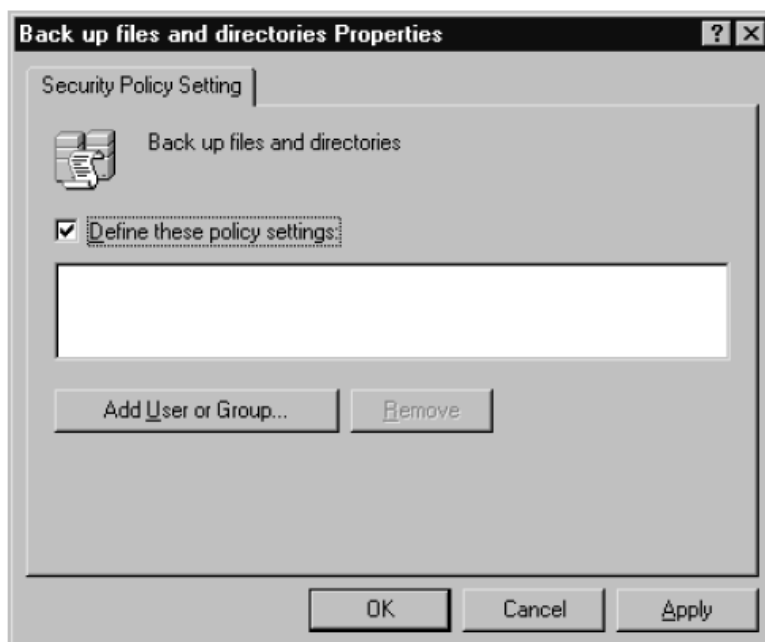
APPLYING USER RIGHTS TO A GROUP

1. Click **Start | Programs | Administrative Tools | Domain Security Policy** to open the Default Domain Security console.



2. Expand the nodes to locate the **User Rights Assignment** node shown.

3. Locate the User Right you wish to define, and double-click it to open it for editing. As seen in Figure, place a check in the **Define these policy settings** option.



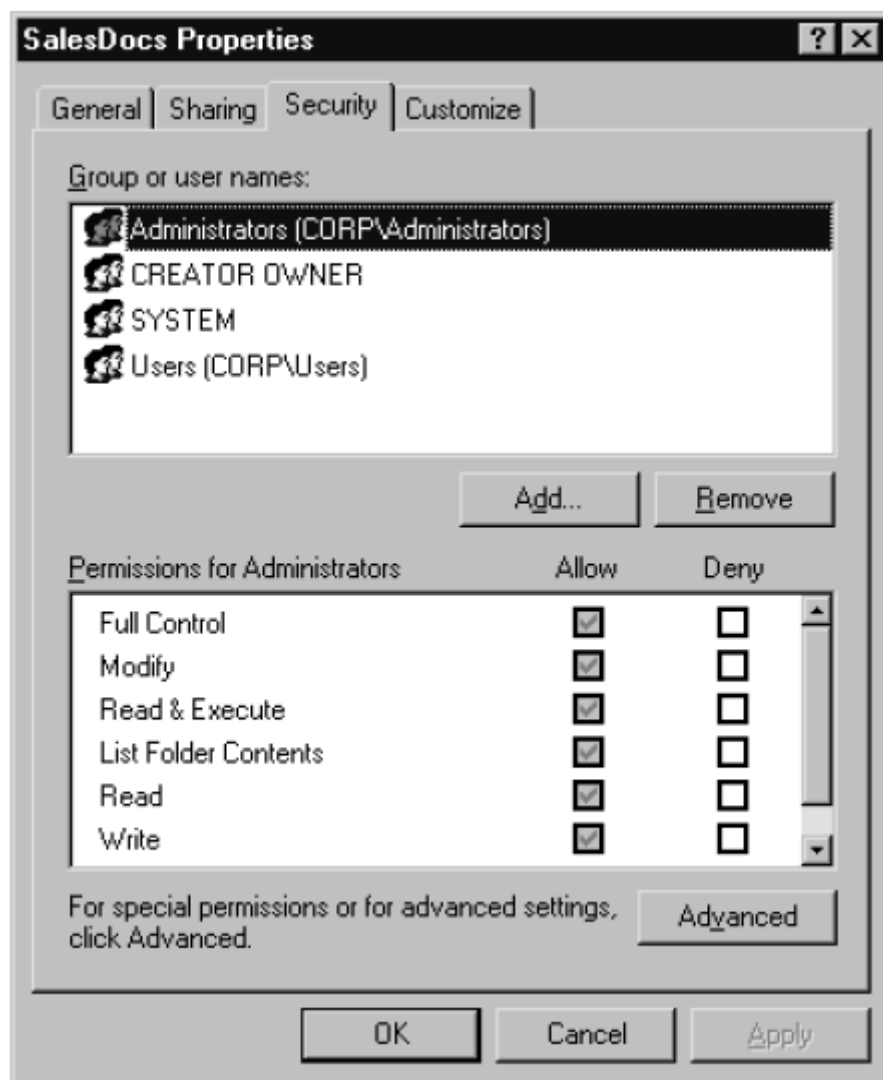
4. Click the **Add User or Group** button to open the Add User or Group dialog box. If you know the name you want to configure the rights for, enter it and click **OK**.

If not, click then click the **Browse** button to open the standard **Select Users, Computers or Groups** dialog box, which will allow you to search for the user or group to add.

More often than not a group is used to simplify the management of access to shared resources on a network. Assigning these permissions takes a different approach than has been seen thus far in our dealings with groups. This is a setting that needs to be configured directly on the object in question, such as a file share or shared printer for example.

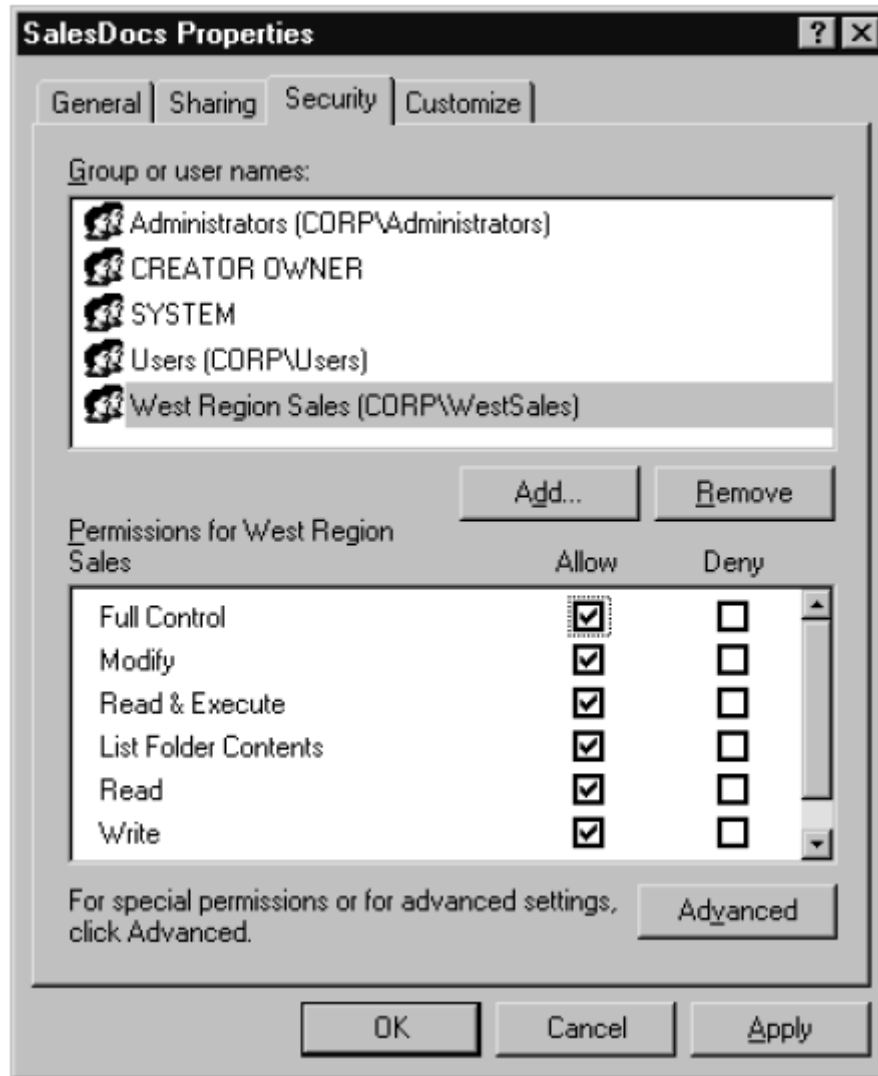
ASSIGNING NTFS PERMISSIONS TO A GROUP

1. Open Windows Explorer and locate the shared resource that you want to configure NTFS permissions on in this example a shared folder.
2. Right-click on the folder and select **Properties** from the context menu.
3. Switch to the **Security** tab as seen in Figure.



4. To add a group to the DACL, click the **Add** button. This opens the Select Users, Contacts, Computers or Groups dialog box as discussed previously.
5. Locate and add the group that you wish to assign permissions to.

6. After adding the group, you will see the results on the **Security** tab, as seen in Figure.



7. Configure the required permissions for the group and click **OK** to accept the changes.

Creating and Managing User Accounts

Up to this point, we have discussed groups only. Groups can be used to collect large numbers of accounts for ease of administration. Networks exist to make the sharing of information easier. As in the previous discussion of groups, the following sections examine user accounts from the perspective of an Active Directory domain environment.

Before discussing creating and managing user accounts, let's examine the default user accounts that are found in the Windows Server 2003 environment.

Default User Accounts

Several default user accounts are created during the installation of Windows Server 2003 and the creation of an Active Directory domain. In the common default user accounts that are created, although several more may be created depending on the specific applications and services installed on the computer.

The Default User Accounts

User Name	User Description
Administrator	A built-in account that is provided for administering the computer and domain. This account is a member of the following groups: Administrators, Domain Admins, Domain Users, Enterprise Admins, Group Policy Creator Owners, and Schema Admins.
Guest	A built-in account that is used for guest access to the computer and domain. This account is a member of the following groups: Domain Guests and Guests. The guest account is disabled by default.
IUSR_computername	A built-in account that is used to allow anonymous access to Internet Information Services (IIS) resources. This account is a member of the following groups: Domain Users and Guests.
IWAM_computername	A built-in account that is used by IIS to start out-of-process applications. This account is a member of the following groups: Domain Users and IIS_WPG.
krbtgt	A built-in account that serves as the Kerberos Key Distribution Center (KDC) service account. This account is a member of the Domain Users group.
SUPPORT_XXXXXXX	A built-in account that is used for the Help and Support Service. This account is a member of the following groups: Domain Users and HelpServicesGroup. The SUPPORT account is disabled by default.

Managing and Modifying User Accounts

It is fairly safe to say that, in most cases, a network administrator will work with user accounts on a daily basis in most networks. Users are the lifeblood of a network the very reason the network exists is to provide information and other resources to users in a secure and efficient way. As such, there are several common tasks to perform when administering user accounts:

Creating new user accounts / **Resetting** a user account password / **Copying** a user account
Disabling or enabling a user account / **Configuring** user account properties / **Deleting** user accounts
Assigning user rights and permissions to a user account

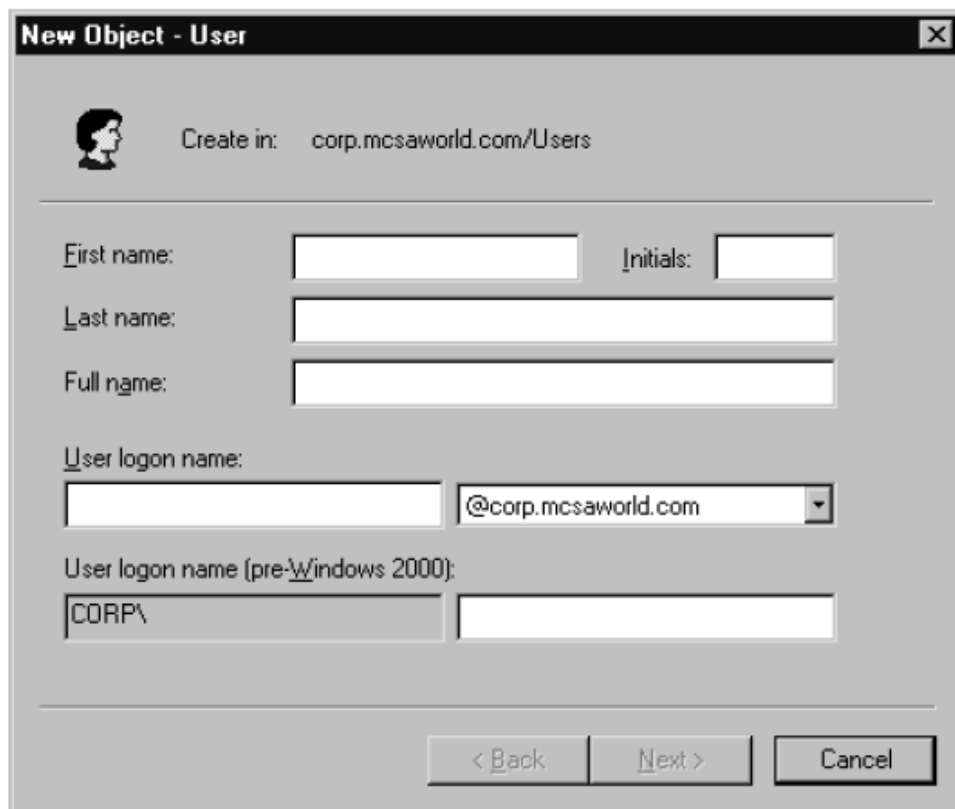
Each of these tasks is discussed in the following sections. We will also examine using two additional command line-based utilities to perform bulk import and export of Active Directory information, including user accounts.

Creating New User Accounts

Creating a new user accounts one at a time is one that can be accomplished from either the Active Directory Users and Computer console or from the command line. The process to create a new user account from the Active Directory Users and Computers console is detailed.

CREATING A NEW USER ACCOUNT WITH AD USERS AND COMPUTERS

1. Open the **Active Directory Users and Computers** console.
2. Right click on the node where you want to create the new user and select **New | User**. The New Object User dialog box opens. Supply the user's name and logon name and click **Next** to continue.



New Object - User

Create in: corp.mcsaworld.com/Users

First name: Initials:

Last name:

Full name:

User logon name: @corp.mcsaworld.com

User logon name (pre-Windows 2000): CORP\

< Back Next > Cancel

4. In the next window supply the password for the user. Good practice dictates that the password assigned here be a temporary one by selecting the **User must change password at next logon** option, which is selected by default. If you are creating an account that is not to be used yet, network security can be increased by disabling it at this time. After entering your selections, click **Next** to continue.



The screenshot shows a 'New Object - User' dialog box. At the top, it says 'Create in: corp.mcsaworld.com/Users'. Below this are two text boxes for 'Password:' and 'Confirm password:'. Underneath these are four checkboxes: 'User must change password at next logon' (checked), 'User cannot change password', 'Password never expires', and 'Account is disabled'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

5. You will be given the chance to review your configuration from a summary page. If all is well, click **Finish** to create the user. You can click **Back** to go back and make changes as required.

Alternatively, user accounts can be created one at a time from the command-line using the *dsadd* command. The specific context to be used to create a new account is:

```
dsadd user UserDN [-UPN UPN] [-samid SAMName] -pwd {Password|*}
```

The *UserDN* and *SAMName* modifiers have been previously explained. The *UPN* modifier specifies the users User Principal Name (UPN), such as *user@mydomain.com*; the *pwd* modifier specifies the account password, or if set as *** specifies that you want to be.

Example to create a new user, Roger Smith, in the Sales OU using the following command:

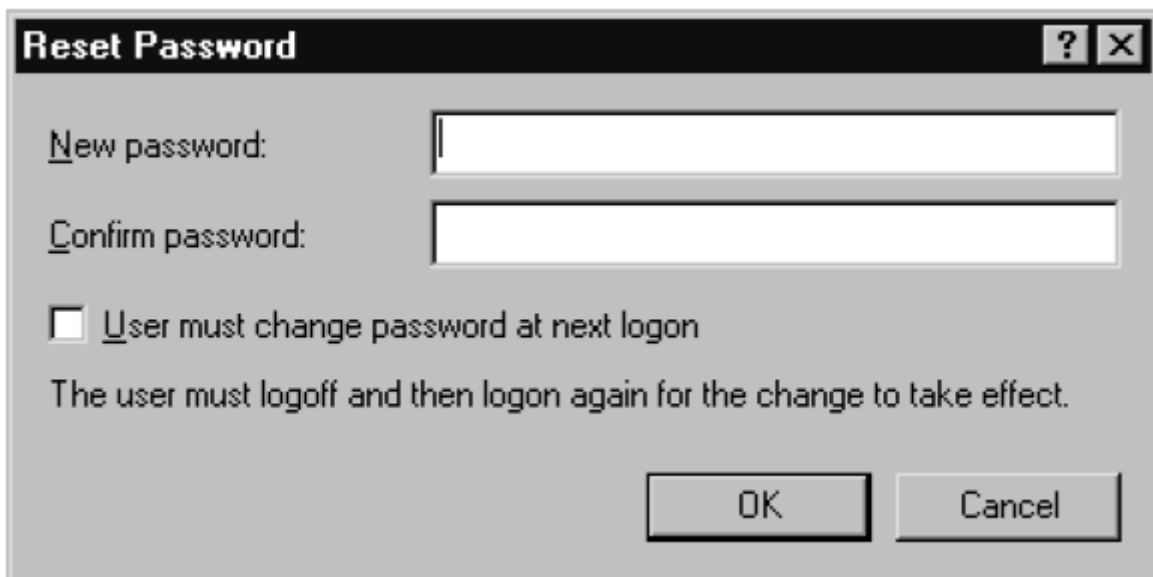
```
dsadd user "CN=Roger Smith,CN=Users,DC=corp,DC=mcsaworld,DC=com" -UPN  
rogersmith@corp.mcsaworld.com -samid rogersmith -pwd *
```

Resetting the User Account Password

It happens more than any administrator wants to talk about: resetting user passwords. In some organizations with particularly challenging password complexity requirements, this can become a burden on network administrators. Even in those organizations where the password policies are not nearly as stringent, users will still forget their passwords. Additionally, the network administrator will oftentimes need to reset the password on an expired or locked out user account. Fortunately, you can quickly and easily reset a user's password from within the Active Directory Users and Computers console.

RESETTING USER PASSWORDS WITH AD USERS AND COMPUTERS

1. Open the **Active Directory Users and Computers** console.
2. Expand the console tree until you locate the user in question.
3. Right-click on the user and select **Reset Password** from the context menu to open the **Reset Password** dialog box seen in Figure.



4. Enter the new password. For enhanced security, select the **User must change password at next logon** option. Click **OK** to reset the user's password.

A user's password can also be easily reset from the command-line using the *dsmod* command with the following syntax: `dsmod user UserDN -pwd NewPassword -mustchpwd {yes|no}`.

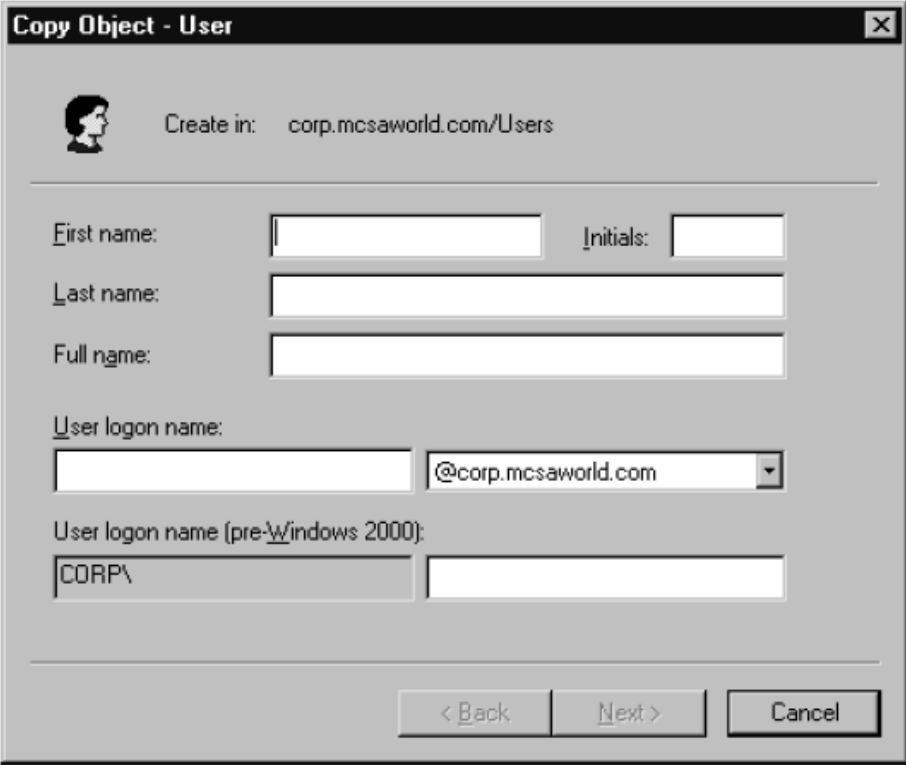
Example using the *dsmod* command to reset the password of user Roger Smith using the following command: `dsmod user "CN=Roger Smith,CN=Users,DC=corp,DC=mcsaworld,DC=com" -pwd * -mustchpwd yes`

Copying a User Account

Many organizations have standardized the way that they create and configure user accounts by creating an *account template*. An account template is nothing more than a user account that has been created and configured in a specific fashion and then used to create new accounts without the administrative burden of needing to configure each new account in a similar fashion. Although the need for this is somewhat offset by the diligent usage of groups and configuring rights and permissions on the group level, there may be the need to copy a user account, creating a new user account with the same features except that the new user account will possess a different SID.

COPYING USER ACCOUNTS FROM AD USERS AND COMPUTERS

1. Open the **Active Directory Users and Computers** console.
2. Expand the console tree until you locate the user in question.
3. Right-click on the user and select **Copy** from the context menu to open the Copy Object User dialog box as seen in Figure.



The screenshot shows the 'Copy Object - User' dialog box. At the top, it says 'Create in: corp.mcsaworld.com/Users'. Below this are several input fields: 'First name:', 'Initials:', 'Last name:', 'Full name:', 'User logon name:' (with a dropdown menu showing '@corp.mcsaworld.com'), and 'User logon name (pre-Windows 2000):' (with a text box containing 'CORP\'). At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

4. You will need to supply the same information for the copy process as you did when creating a new user account. By default, only the most common attributes are copied during the user account copy process. These include log on hours, workstation restrictions, and account expiration date. You can modify which attributes are copied to the newly created user from the Active

Disabling or Enabling A User Account

A network administrator may need to disable a user account for any number of reasons. Commonly, they will disable user accounts when the user is gone for an extended period of time, or as a security measure to keep unused accounts from becoming a weakness in their network security plan. The administrator can quickly disable a user account from the Active Directory Users and Computers console by right-clicking on the account and selecting **Disable Account** from the context menu. Similarly, they can enable a disabled user account by right-clicking on the account and selecting **Enable Account**. They can also disable or enable a user account from the Account tab on the Properties dialog.

An account can also be disabled or enabled from the command-line using the *dsmod* command with the following syntax: **dsmod user UserDN -disabled {yes|no}**.

Configuring User Account Properties

When user accounts are created using the Active Directory Users and Computers console or using the minimum required command syntax of the *dsadd* command, many user attributes and information items still need to be configured. Most of these items can be configured using the *dsadd* command at the time of account creation, or the *dsmod* command after the fact. The following sections examine the configuration process entirely from the Active Directory Users and Computers console.

Within Active Directory Users and Computers, locate the user account that you wish to configure account properties for and double-click it to open the Properties dialog box.

The General Tab

The General tab of the account Properties dialog box, seen in Figure, allows the network administrator to configure basic user information such as first and last name, display name, a description of the account, office location, telephone number, e-mail address, and Web page information.

The screenshot shows the 'Roger Smith Properties' dialog box with the 'General' tab selected. The dialog has a title bar with a question mark and close button. Below the title bar are several tabs: Member Of, Dial-in, Environment, Sessions, Remote control, Terminal Services Profile, COM+, General, Address, Account, Profile, Telephones, and Organization. The 'General' tab is active, showing a user icon and the name 'Roger Smith'. The fields are as follows:

Field	Value
First name:	Roger
Initials:	
Last name:	Smith
Display name:	Roger Smith
Description:	
Office:	Arizona Sales
Telephone number:	480-555-9876
E-mail:	rogers@mcsaworld.com
Web page:	http://www.mcsaworld.com

At the bottom are buttons for OK, Cancel, and Apply.

The Address Tab

The Address tab of the account Properties dialog box, seen in Figure, allows the network administrator to configure a complete mailing address for the user.

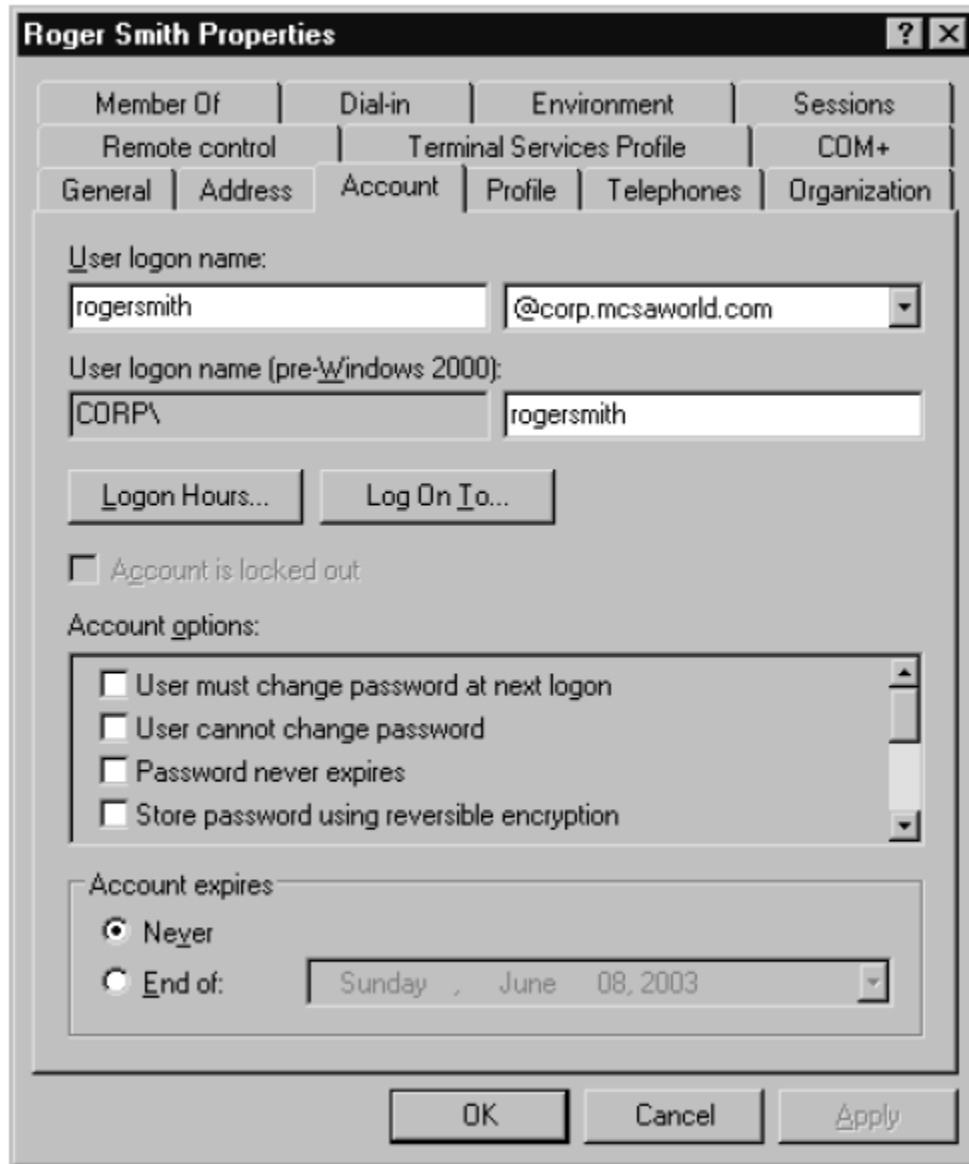
The screenshot shows a Windows-style dialog box titled "Roger Smith Properties". It has a tabbed interface with the following tabs: "Member Of", "Dial-in", "Environment", "Sessions", "Remote control", "Terminal Services Profile", "COM+", "General", "Address", "Account", "Profile", "Telephones", and "Organization". The "Address" tab is currently selected. The dialog contains several input fields for a mailing address:

- Street:** A text box containing "789 My Avenue".
- P.O. Box:** An empty text box.
- City:** A text box containing "Any Town".
- State/province:** A text box containing "AZ".
- Zip/Postal Code:** A text box containing "85555".
- Country/region:** A dropdown menu showing "United States".

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

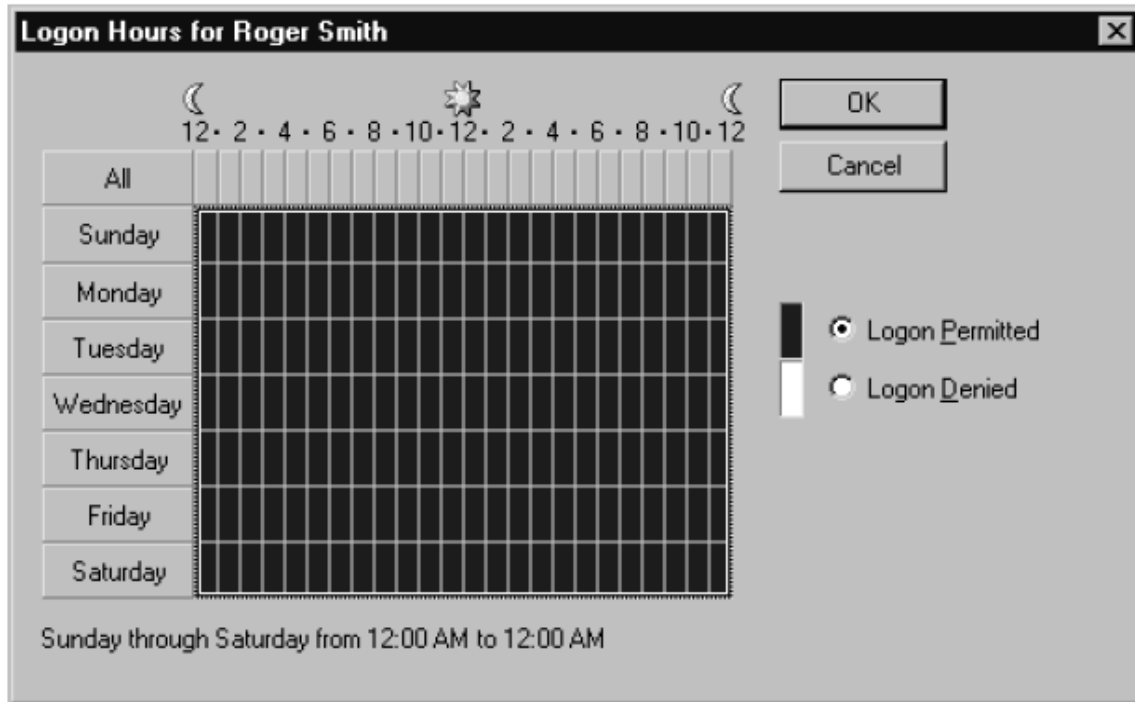
The Account Tab

The Account tab of the account Properties dialog box, seen in Figure, allows the network administrator to modify account attributes such as the logon name, the pre-Windows 2000 log-on name, logon hours, logon location restrictions, account expiration date, and several other account options.



CONFIGURING USER LOGON TIME AND COMPUTER RESTRICTIONS

1. On the **Account** tab of the user Properties dialog box, click the **Logon Hours** button to open the Logon Hours for User dialog box, seen in Figure.



2. Blue squares represent those times when a user is allowed to logon to the network, while white squares represent those times when the user is not allowed to logon. By default, logon is allowed 7 days per week, 24 hours per day.

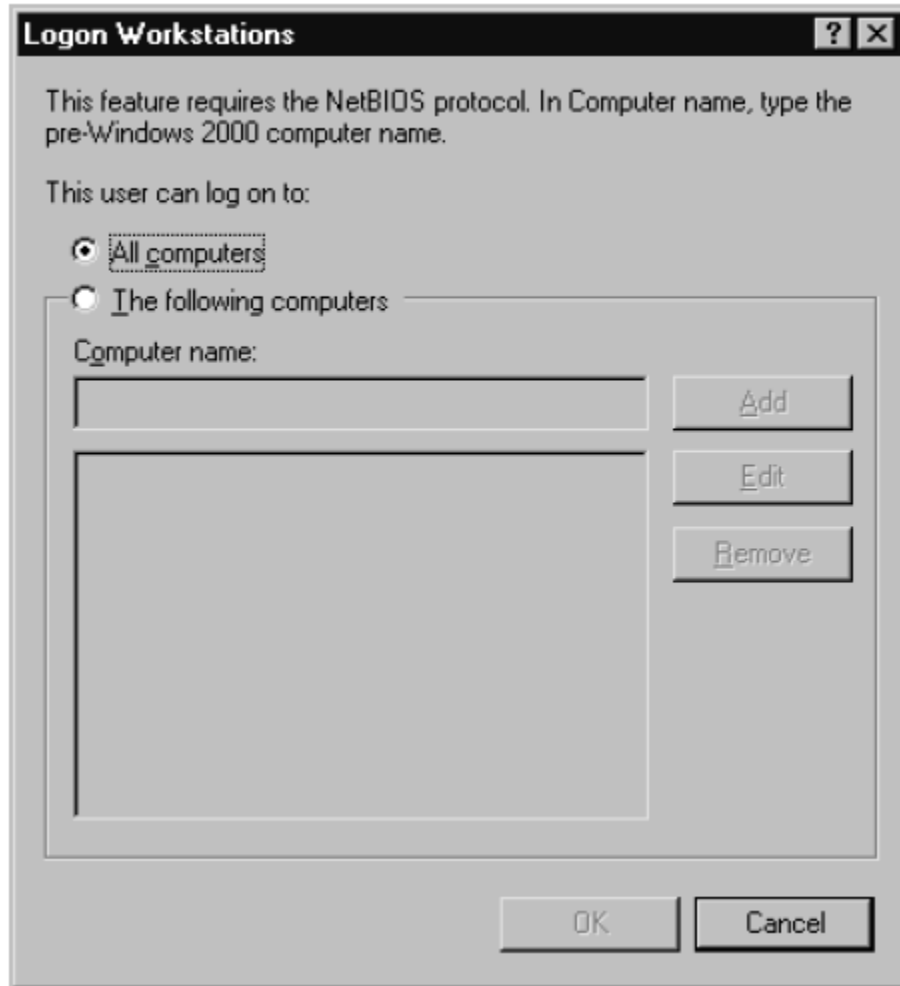
3. To configure a log-on hours restriction, click the **Logon Denied** button.

4. Select a starting day and time (Monday, 6 A.M. for example) and drag the cursor to highlight the time you wish to allow logon. Click the **Logon Permitted** button to make the changes. In this example, Roger Smith will now be allowed to logon only during the time period of Monday – Friday, from 6 A.M. – 6 P.M.

5. Click **OK** to accept the changes.

6. To configure a log-on computer restriction, which will limit the computers the user can logon to the network from, click the **Log On To** button on the **Account** tab of the user **Properties** dialog box.

7. The Logon Workstations dialog box will open allowing you enter the NetBIOS names of the computers this user will be allowed to logon in from.



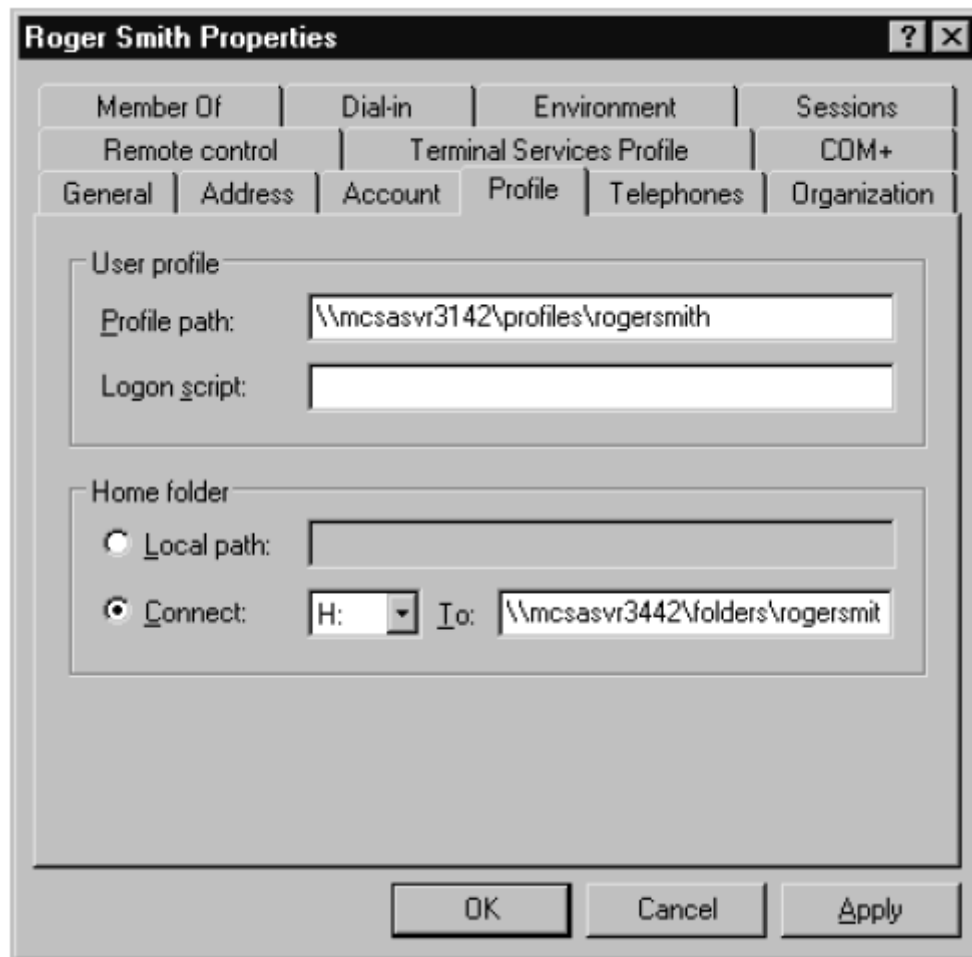
8. To enter computer names, select the **The following computers** button.

9. Enter the NetBIOS computer name, such as MCSAWKS042, for each computer that is to be allowed user logon. Note that the NetBIOS computer name MCSAWKS042 would belong to the computer with the following Fully Qualified Domain Name (FQDN) in this example domain: MCSAWKS042.corp.mcsaworld.com.

10. Click OK to accept the logon computer restrictions

The Profile Tab

The Profile tab of the account Properties dialog box, seen in Figure 1.44, allows the network administrator to specify a profile path, logon script, and home folder for the account.



The Telephones Tab

The Telephones tab of the account Properties dialog box, seen in Figure allows the network administrator to enter several different telephone numbers for a user including home, fax, pager, and mobile and IP phone numbers.

The Organization Tab

The Organization tab of the account Properties dialog box, allows the network administrator to configure title and departmental information about the user. Additionally, they can enter the user's supervisor. On the Organization tab of the selected supervisor, the user's name will appear in the Direct reports area.

Deleting User Accounts

Occasionally, user accounts must be deleted, most commonly when a user no longer works for an organization. It is important to delete an inactive user account as soon as possible.

For example, company policy might dictate that user accounts are to be disabled starting the day a user leaves the company. After 45 days if the user has not returned to the company, the user account is deleted to prevent its misuse

DELETING USERS FROM AD USERS AND COMPUTERS

1. Open the **Active Directory Users and Computers** console.
2. Expand the console tree until you locate the user to be deleted.
3. Right-click on the user and select **Delete** from the context menu.
4. When prompted if you want to delete the user, click **Yes**.

A user account can be deleted from the command-line using the *dsrm* command with the following syntax: **dsrm ObjectDN**.

Example using the *dsrm* command to delete the user account of Roger Smith using the following command: `dsrm "CN=Roger Smith,CN=Users,DC=corp,DC=mcsaworld,DC=com"`

Creating and Managing Computer Accounts

Computer accounts serve the same basic function as user accounts: they are used to determine the rights and permissions that a computer will have in the domain. Although computer accounts can be created for any Windows computer on a network, only Windows 2000 or better computers will be able to fully participate in Active Directory and receive security and management configuration from Active Directory. Windows 9x and Windows NT computers will require the use of System Policies to configure security and management options. You can learn more about System Policies at

www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/tattooing.asp.

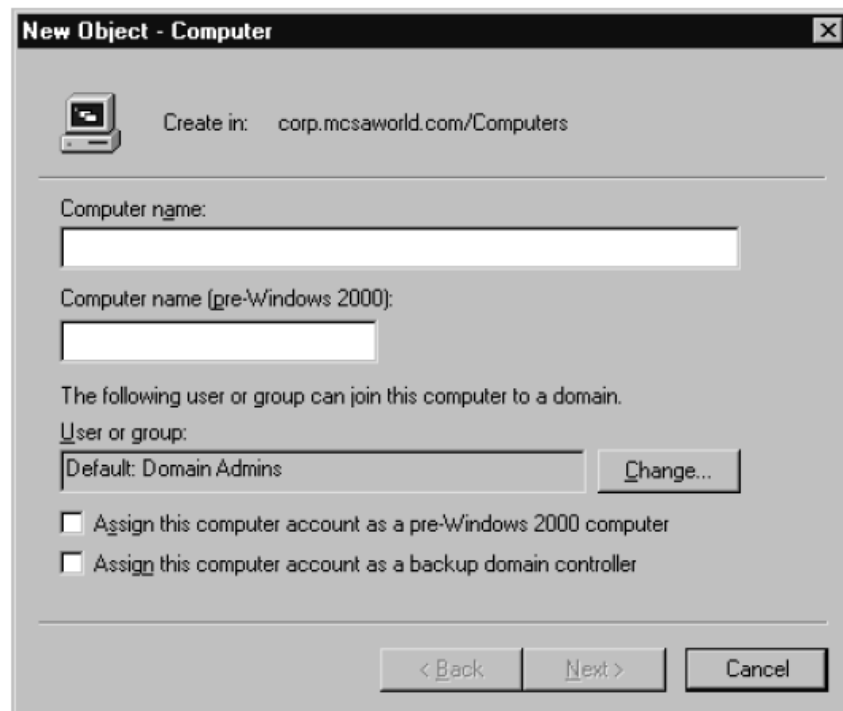
Computer accounts can be created in one of two ways: manually through usage of the Active Directory Users and Computers console or from the command-line, or automatically by joining a Windows 2000, Windows XP, or Windows Server 2003 computer to a domain. Each of these events is examined in more detail in the following sections.

Creating and Modifying Computer Accounts Manually

Computer accounts can be manually created in much the same fashion as user accounts. A network administrator can create a computer account from the Active Directory Users and Computers console, or from the command-line as desired.

CREATING COMPUTER ACCOUNTS FROM AD USERS AND COMPUTERS

1. Open the **Active Directory Users and Computers** console.
2. Expand the console tree until you locate the location in which you wish to create the new computer.
3. Right-click on the node and select **New | Computer** from the context menu to open the New Object – Computer dialog box, seen in Figure



4. Enter the computer name and pre-Windows 2000 information. If this is a pre-Windows 2000 computer, select the appropriate option. If this computer is a Windows NT 4.0 BDC, select the appropriate option.

After making your selections, click **Next** to continue.

5. On the Managed page, seen in Figure 1.50, click **Next** to continue without making any configuration changes. You would only need to enter information in this location if the computer were being prestaged for Remote Installation Service (RIS) installation of an operating system.



6. From the summary page, click **Finish** to complete the computer account creation process.

Computer accounts can also be created from the command-line by using the *dsadd* command with the following syntax: **dsadd computer ComputerDN**

Example using the *dsadd* command to create the computer account for a computer with a NetBIOS name of A51WXP3142 in the Sales OU using the following

command: **dsadd computer CN=MCSAWXP3142,CN=Computers,DC=corp,DC=mcsaworld,DC=com**

Creating Computer Accounts by Joining to the Domain

As an alternative to creating a computer account manually, a network administrator may also create a computer account automatically by joining the computer to a domain.

JOINING A COMPUTER TO THE DOMAIN

1. On the computer to be joined to the domain, log on using an account that has local Administrative credentials.
2. Open the **System** applet in the Control Panel and click on the **Network Identification** tab.
3. Click the **Properties** button to open the Identification Changes dialog box seen in Figure 1.52. As seen in this example, this computer is currently part of a workgroup.



4. Select the **Domain** button, enter the domain name that the computer is to be joined to, and click **OK**.

You will be prompted for the credentials of a user authorized to add computers to the domain. Supply them as seen in Figure.

6. Click **OK**. After some delay, depending on network conditions, you will receive the Welcome dialog box seen in Figure.



7. Click **OK** to acknowledge the successful joining. You will be informed that you will need to restart the computer to complete the process.

8. Close the System applet and restart the computer.

9. When you log on next time from that computer, you will be logging onto your domain.

Frequently Asked

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the Exam Objectives presented in this chapter, and to assist you with real-life implementation of these concepts. You will also gain access to thousands of other FAQs at ITFAQnet.com.

Q: It seems like creating groups, assigning them user rights and permissions, and then placing users in the groups is an awful lot of work. Why can't I just manage the user rights and permissions directly on the users themselves?

Q: I have an employee that just quit the company last week. Should I delete her user account from Active Directory?

Q: Why would I ever want to rename a user account and reassign it to another user?

Q: How can I use the command line utilities to quickly create large numbers of user accounts?

Q: How can the *csvde* and *ldifde* tools help me?

Q: Do all Active Directory manipulations have to be performed locally on a domain controller?

Test**Creating and Managing Groups / User Accounts / Computer Accounts**

1. You are an assistant network administrator for Billy's Jeans, Inc. You have been tasked with creating three new groups, one for each of the following divisions: Sales, Marketing, and Production. The Sales group is to be configured with permissions required to access a shared network folder named Sales. The Marketing group is to be configured only for e-mail distribution to its members. The Production group is to be configured for both e-mail distribution and with the required permissions to access the Sales folder. Which of the following set of actions presents the correct steps to accomplish the requirement you have been tasked with?

A. Create a security group named Sales and configure the Sales folder with the required permissions for this group. Create a security group named Marketing and configure the Sales folder with the required permissions for this group. Create a distribution group named Production and configure the Sales folder with the required permissions for this group. Additionally, configure an e-mail address for the Production group.

B. Create a distribution group named Sales and configure the Sales folder with the required permissions for this group. Create a distribution group named Marketing and configure an e-mail address for this group. Create a security group named Production and configure the Sales folder with the required permissions for this group. Additionally, configure an e-mail address for the Production group.

C. Create a security group named Sales and configure the Sales folder with the required permissions for this group. Create a distribution group named Production and configure an e-mail address for this group. Create a security group named Marketing and configure an e-mail address for this group.

D. Create a security group named Sales and configure the Sales folder with the required permissions for this group. Create a distribution group named Marketing and configure an e-mail address for this group. Create a security group named Production and configure an e-mail address for this group. Additionally, configure the Sales folder with the required permissions for the Production group.

2. Hannah is preparing to configure user rights and permissions for 1,600 users that are spread out over five different departments: Sales, Marketing, Production, Engineering, and Administration. Each department is composed of two divisions: East and West. The network is also composed of two child domains under the root domain: East and West. The network has a total of ten divisions. How can Hannah create groups to use in assigning user rights and permissions without causing excessive directory replication between the two child domains? (Choose two correct answers)

A. Hannah should create universal groups for all ten divisions.

B. Hannah should create two universal groups, UEast and Uwest, and place the five respective departmental groups in them.

C. Hannah should create global groups for all ten divisions.

D. Hannah should create two global groups, GEast and Gwest, and place the five respective departmental groups in them.

3. You are preparing to assign user rights and permissions to 150 users on your network. Which of the following reasons explain why assigning the rights and permissions to a group and then placing the users into the group is the best course of action? (Choose three correct answers)

A. Configuring user rights and permissions on groups is more accurate than configuring user rights and permissions on individual user accounts.

B. Configuring user rights and permissions on groups requires less administrative time and labor to perform.

C. Configuring user rights and permissions on groups allows you to quickly manage which users get these rights and permissions by adding or removing them from the group.

D. Configuring user rights and permissions on groups prevents attackers from using the user accounts in an unauthorized fashion.

4. Austin is attempting to create a new group for his network that he wants to place several global groups into. When he tries to create the new group as a universal group, the option to do so is not available. What is the most likely reason for this problem?

- A.** Austin's domain is operating in the Windows NT 4.0 native functional mode.
- B.** Austin's domain is operating in the Windows 2000 mixed functional mode.
- C.** Austin's domain is operating in the Windows Server 2003 functional mode.
- D.** Austin's domain is operating in the Windows 2000 native functional mode.

5. Andrea has created a new security group for several help desk staff in her company. She has configured the required user rights and permissions on this security group and placed the help desk staff user accounts into the group. When Andrea tries to send an e-mail message to the security group, she gets a bounce back informing her that no such user was found. What is the most likely reason for this problem?

- A.** One of the users in the group is not mailbox enabled.
- B.** The group does not have an e-mail address configured for it.
- C.** The group is not a distribution group.
- D.** None of the users in the group are mailbox enabled.

6. Jon is creating several dozen new domain local security groups for his network. What command line utility could Jon use to create these groups for him?

- A.** `dsadd group GroupDN -secgrp yes -scope l -samid SAMName -desc Description`
- B.** `dsadd group GroupDN -secgrp yes -scope g -samid SAMName -desc Description`
- C.** `dsadd group GroupDN -secgrp no -scope l -samid SAMName -desc Description`
- D.** `dsadd group GroupDN -secgrp yes -scope u -samid SAMName -desc Description`

7. You have been tasked with determining the group membership status of several hundred employees within your organization. You have determined that it would be more efficient to perform this task from the command line. Which command line utility can be used to determine which groups a specified user is a member of?

- A.** `dsquery` / **B.** `dsget` / **C.** `dsmod` / **D.** `dsrm`

8. Andrew is a member of the help desk staff for Tim's Tents, Inc. Where can Andrew look to determine what groups that a user is a member of from within the Windows GUI?

- A.** The Member Of tab in the group Properties dialog box.
- B.** The Member Of tab in the user Properties dialog box.
- C.** The Account tab in the user Properties dialog box.
- D.** The Managed By tab in the group Properties tab.

9. Which of the following user accounts is used to provide anonymous access to IIS resources and is a member of the Domain Users and Guests groups?

- A.** `IWAM_computername` / **B.** `SUPPORT_XXXXXXXX` / **C.** `IUSR_computername` / **D.** `krbtgt`

10. You have just completed a clean installation of Windows Server 2003 on a new server in your organization. Several default user accounts are created by the installation process. Which of the following default users are disabled by default? (Choose two correct answers.)

- A.** Administrator / **B.** Guest / **C.** `IUSR_computername` / **D.** `SUPPORT_XXXXXXXX`

11. You are in the process of creating new user accounts from the command line using the `dsadd` command. If the `pwd *` modifier is specified, what is the net result?

- A.** The password is to be randomly assigned. / **B.** The password is to be left blank.

C. The password is to be taken from another list. / D. The password is to be supplied during the creation process.

12. You are a help desk staff member for your organization. A member of the Advertising department has requested that her password be changed. Which of the following items of information will you need to know in order to reset the password for her?

- A. The user's current password. / B. The user's e-mail address.
- C. The user account name. / D. The user's supervisor's name.

13. Which of the following computers can have computer accounts in Active Directory? (Choose all correct answers.)

- A. Windows 2000 Professional / B. Windows XP Professional
- C. Windows 98 / D. Windows 95

14. In what two ways can computer accounts be created in Active Directory? (Choose two correct answers.)

- A. By joining a Windows 95 computer to the domain.
- B. By joining a Windows 2000 Professional computer to the domain.
- C. Through manual creation from Active Directory Sites and Services.
- D. Through manual creation from Active Directory Users and Computers.

15. Chris is preparing to import a CSV file containing data from another LDAP-compliant directory service into the Active Directory of her domain. What is the minimum command that she will need to issue to perform the importation of the data in the file named userlist.csv?

- A. `csvde -f filename` / B. `ldifde -i -f filename` / C. `csvde -i -f filename` / D. `csvde -i`

Extended Command Line Functionality

Some of the biggest improvements in Windows Server 2003 are the significant enhancements made to the command line utilities. The following new command line tools have been added to make the administrator's job easier:

dsadd Can be used to add new objects into Active Directory such as contacts, computers, groups, organizational units, and users.

dsmod Can be used to modify an existing object in Active Directory.

dsrm Can be used to remove an existing object from Active Directory.

dsmove Can be used to move a single object in Active Directory within the same domain from one location to another. Can also be used to rename an object without moving it.

dsquery Can be used to query Active Directory per the specified criteria to locate a specific object or object type.

dsget Can be used to display the properties of a specific object in Active Directory.