

3

CHAPTER THREE

Managing Groups

Objectives

This chapter covers the following Microsoft-specified objectives for the “Managing Users, Computers, and Groups” section of the Managing and Maintaining a Microsoft Windows Server 2003 Environment exam:

Create and manage groups

- ▶ **Create and modify groups by using the Active Directory Users and Computers console.**
- ▶ **Identify and modify the scope of a group.**
- ▶ **Manage group membership.**
- ▶ **Find domain groups in which a user is a member.**
- ▶ **Create and modify groups by using automation.**
- ▶ For simplicity of network administration, we can create group objects and allocate resource access rights to these objects. Then by making user accounts members of the group, we can grant them the access that the group objects have been assigned.

Outline

Introduction	126	Chapter Summary	153
		Key Terms	153
Creating and Managing Groups	126	Apply Your Knowledge	153
The Four Domain Functional Levels	127		
The Three Forest Functional Levels	128		
Group Type	129		
Group Scope	129		
Domain Local Groups	131		
Global Groups	132		
Universal Groups	132		
Recommended Sequence of Groups	133		
Default Groups	134		
Default Groups on Member Servers	134		
Default Groups in Active Directory	136		
System Groups	137		
Creating and Modifying Groups by Using the Active Directory Users and Computers Console	138		
Identifying and Modifying the Scope of a Group	142		
Managing Group Membership	144		
Adding Accounts to Groups with Command-Line Tools	146		
Finding Domain Groups in Which a User Is a Member	148		
Creating and Modifying Groups by Using Automation	149		
Assigning Groups	151		

Study Strategies

- ▶ In studying this section, be sure to practice all the activities described. Become very familiar with Active Directory Users and Computers and creating groups.
- ▶ Examine the use of the default groups. Know their capabilities and limitations.
- ▶ You will need access to a Windows Server 2003 domain controller. Many of the tools are new, or they differ from those available in Windows 2000, so don't try to get by with a Windows 2000 domain controller.
- ▶ Memorize the AGDLP acronym and what it means. It is a best practice that will serve you well, both on the exam and on the job.

Introduction

This chapter continues your study of some of the common daily duties of a Windows Server 2003 administrator. You can rest assured that you will perform the tasks you learn in this chapter very often. This chapter discusses creating and managing group accounts, including what type of group to use for particular situations. An especially important topic is group scope, as well as how it is affected by domain functional level. We'll be starting with creating and managing groups. Let's get to it!

Creating and Managing Groups

Objective:

Create and manage groups

It's much easier to administer a network when you can manage several users at once. We can expect that all members of a given section of an organization will have the same needs in accessing data or using printers, and it's also likely that they should be subject to the same security restrictions. Rather than granting individual users the rights to print to a particular printer or to update files in a given folder, we can allocate those rights to a group object.

With users belonging to groups, you can allocate resource access permissions to the group one time rather than individually to each user in that group. For example, you might have 50 members of a human resource group. You can individually grant access to human resource files and folders to the 50 members, but that obviously could take a long time and leave you open to committing an error that potentially could breach the security of highly sensitive human resource data. Now, if you create a human resource group and add the 50 human resource members to the group, you can configure the necessary access levels to all 50 human resource users at one time by configuring the proper access permissions to the group. It's a one-time action that takes care of 50 individuals!

Making user accounts members of the group automatically grants them any rights that group object has. Therefore, it is useful to create groups, allocate members to those groups, and grant resource access permissions to the groups.

Windows Server 2003 has a number of ways of defining groups of user accounts. We'll describe the different methods a little later, but first you have to understand that Windows Server 2003 domains can be in four different functional levels, and those levels impact what types of groups are possible and what nesting of those groups can be done. (The functional levels have implications related to other capabilities as well, such as Active Directory replication efficiencies, but we're interested only in group behavior here.)

The Four Domain Functional Levels

When the Windows Server 2003 version of Active Directory is installed, a basic set of features is enabled that allows the new domain controller to retain backward compatibility with older domain controllers running Windows NT 4.0 or Windows 2000. As these older domain controllers are removed from the network, the administrator can enable the additional features by raising the domain functional level. The domain functional level determines what features are available and whether older domain controllers are supported. Here are the four domain functional levels:

NOTE

Active Directory Functional Levels In fact, several capabilities are available only in the Windows Server 2003 functional level, including improved Active Directory replication and schema handling. For the exam, we're interested only in the effect the domain functionality level has on groups.

- ▶ *Windows 2000 mixed*—The default level in Windows Server 2003, this level is equivalent to mixed mode in Windows 2000. At this level, a domain can contain domain controllers on computers running Windows NT, Windows 2000, or Windows Server 2003. This flexibility comes with a price, as you'll see, because at this level you cannot use the enhanced group features available in either Windows 2000 or Windows Server 2003.
- ▶ *Windows 2000 native*—After you have removed all Windows NT domain controllers from the domain, you can increase the domain functionality level to Windows 2000 native. At the Windows 2000 native level, you get the improved group capabilities of Active Directory as delivered in Windows 2000, such as the capability to “nest” groups and the availability of groups of Universal scope.
- ▶ *Windows Server 2003 interim*—Both Windows NT and Windows Server 2003 domain controllers can exist in a domain at this level. As with the Windows 2000 mixed level, enhanced group functionality cannot be used.
- ▶ *Windows Server 2003*—Only domains that have no Windows 2000 or Windows NT domain controllers can be raised to this level of domain functionality. This is the most advanced level of domain functionality. Although important enhancements are achieved in upgrading from Windows 2000 to Windows Server 2003 Active Directory, there are no significant differences in group functionality between the two levels.

Figure 3.1 shows raising the domain functional level using the Active Directory Users and Computers Microsoft Management Console (MMC).

CAUTION

Raising Functional Levels This step is not reversible, so it should be initiated on a production network only by an experienced network administrator.

EXAM ALERT

Expect Functional Level Questions Expect several exam questions that deal with the topic of the different features enabled at different functional levels.

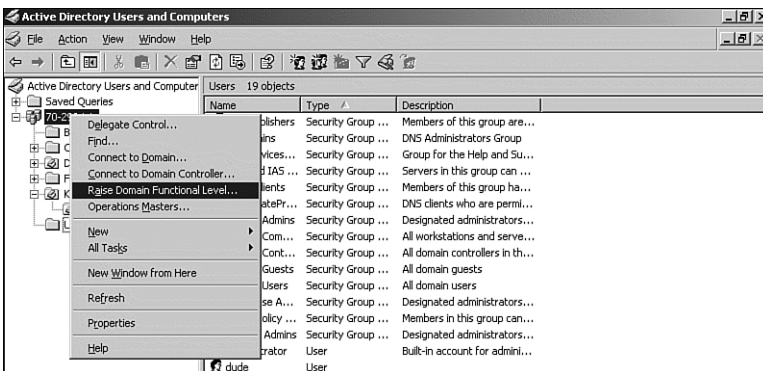


FIGURE 3.1 Raising the domain functional level.

The Three Forest Functional Levels

If you remember when we were promoting our member server to a domain controller, we were prompted as to whether to create a new Forest. A Forest is a logical construct within Active Directory. Logical in that you really can't see or manage it. The forest encompasses all the objects, domains, organizational units (OUs), and so on within it. By default, all domains created in a forest are linked together via transitive trusts so that the administrator has the option of granting access to resources in his or her domain to users and groups in other domains.

Although you can expect forests to be covered at length in other exams, for this one, you will only need to know the following:

- ▶ *Windows 2000 forest*—The default level in Windows Server 2003, this level is equivalent to mixed mode in Windows 2000. At this level, a domain can contain domain controllers on computers running Windows NT, Windows 2000, or Windows Server 2003. At this level, each group can contain no more than 5,000 accounts. This level is the default with a new installation.
- ▶ *Windows Server 2003 interim forest*—Only Windows NT and Windows Server 2003 domain controllers can exist in a forest at this level. As with the Windows 2000 level,

enhanced group functionality cannot be used. This level is the default when upgrading from Windows NT 4.0.

- ▶ *Windows Server 2003 forest*—Only forests that have no Windows 2000 or Windows NT domain controllers can be raised to this level of forest functionality. This level enables support for groups containing more than 5,000 members.

Figure 3.2 shows raising the forest functional level using the Active Directory Domains and Trusts MMC.

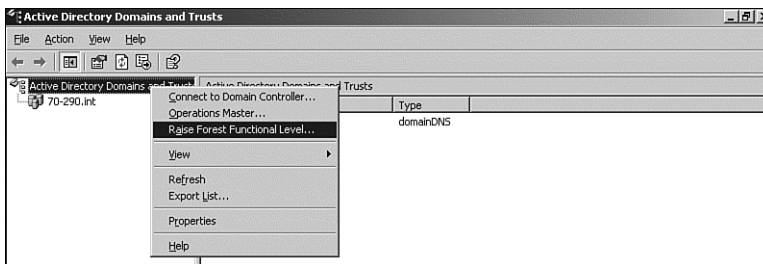


FIGURE 3.2 Raising the forest functional level.

Group Type

The two types of groups are *distribution groups*, which are used only for email lists, and *security groups*, which can be used both for email distribution and resource access. You choose the type depending on the reason you are creating the group:

- ▶ *Distribution Groups*—Used for email distribution lists only. Cannot be assigned permissions to use resources.
- ▶ *Security Groups*—Used both for assignment of permissions to use resources and for email distribution.

Group Scope

Objective:

Identify and modify the scope of a group

The second way of classifying a group is by defining its *scope*. Group scope means determining where the group members and the resources that the group can be granted access permissions to reside. Table 3.1 lists the scope of the group object in the first column (domain local, Global, and Universal); in the second column, the object types that can be members of this kind of group; in the third column, the locations of the resources that a group can be given access to.

Note that in several cases, the characteristics of the group object differ depending on the functionality of the domain.

TABLE 3.1 Group Scopes and Applicable Members and Rights

Scope	Can Include	Can Be Granted Access to Resources In
domain local	Accounts, global groups, and universal groups from any domain, and, in Windows 2000 native or Windows Server 2003 functional level domains, other domain local groups from the same domain as the group object.	The local domain
Global	In domains at the Windows 2000 mixed level or at the Windows Server 2003 interim level, only accounts from the same domain as the group object. In Windows 2000 native or Windows Server 2003 functional level domains, accounts and other global groups from the same domain as the group object.	Any domain in the forest and any domain in any other forest that trusts the local domain
Universal	(Not available in domains at the Windows 2000 mixed level or the Windows Server 2003 interim level.) Accounts, global groups, and universal groups from any domain.	Any domain in the forest and any domain in any other forest that trusts the local domain

How would you choose the scope of a group you need to create? Let's talk about each scope in turn.

EXAM ALERT

Understand Groups and Scope Expect at least one exam question that deals with the scope of groups in Windows Server 2003. Microsoft has always tested heavily on the different types of groups and their scope. This exam will probably not be any different.

Domain Local Groups

Groups of the domain local scope are typically used for resource access. When creating a group of this scope, you think of the resource that we're granting access to, rather than the users who might use the resource. You also name the group object after the resource. You might create a domain local group with the name DL-PhoenixEngineeringResources, for example. You would grant this group Read and Write access to the folders and printers that are used by engineers in Phoenix. The members of the group can be (refer back to Table 3.1) user accounts, global groups, and universal groups from any domain trusted by this domain.

NOTE

Scope of Trusts A domain trusts all other domains in its forest and any other domains that the administrator has explicitly set the domain to trust. Trusts are covered on the 70-294 exam.

If the domain is at the Windows 2000 native functional level or the Windows Server 2003 functional level, the new group can also have other domain local group accounts among its members. The capability to make a group a member of another group of the same type is called *nesting*.

NOTE

Nesting Groups The capability to nest groups is very useful in administration. With nesting, you could define a DL-PhoenixUsers group, whose members are groups called DL-PhoenixPersonnel, DL-PhoenixEngineers, and DL-PhoenixHR. You would make the user accounts members of the departmental groups, with no need to also make them members of the city group.

We have just listed the types of objects that can be members of our new domain local group, but what types are we likely to use? Typically, the member list of a domain local group includes an administrator account and one or more global group accounts. More rarely, you may also see universal group accounts in the domain local group member list.

NOTE

Local Versus Domain Local It's easy to confuse domain local groups with local groups. Local groups are the groups that are resident on a server and have no visibility in the domain. Although they can be used to grant access to resources on that server, you will have to log on or connect to that server to work with them. Domain local groups are stored and managed by Active Directory; therefore, they are visible throughout the domain. However, they are not visible in other domains. We discuss local groups in the upcoming section, "Default Groups."

Global Groups

A *global group* is used to collect user accounts, typically according to the function the members perform in their work. Therefore, their names reference the accounts that are on the group member list—typical global group names are G-PhoenixEngineers and G-KansasCityHR. Only accounts in the same domain as the group object can be members of the global group. The reason the group is called “global” is that the group can be assigned access to any resource or made a member of any domain local group in the entire forest.

Identifying Groups

You’ve probably noticed that we’ve been prefixing group names with “DL-” or “G-.” This is a shorthand way of identifying the group type, so that we know what the scope of the group is at a glance. For the short scenarios we cover in this book, it’s probably not necessary, but in the real world, it can save a lot of time, especially when troubleshooting a permissions problem. Will you remember the type of a group you or your co-workers created six months ago?

If the domain is at the Windows 2000 native functional level or the Windows Server 2003 functional level, the new group can also have other global group accounts from its domain among its members.

A good example of the use of global groups is when users are disbursed and resources exist in few domains. For example, an engineering company has engineers in its Kansas City, Phoenix, and Chicago offices. Each location hosts its own domain in a Windows Server 2003 Active Directory forest. All engineering resources are located in the Phoenix domain. Each domain administrator places his engineers in an “engineers” Global group for his domain. The Phoenix domain administrator creates the EngRes domain local group and assigns the selected permissions to that group. He then places each Engineers Global group from each domain into the EngRes group. The Phoenix administrator relies on the other administrators to determine who in their respective domains is allowed access to the resources.

Universal Groups

A *universal group*, as its name implies, has no limitations as to where its members are located, or in what domains it can be granted resource access. Its members can come from any trusted domain, and it can be a member of any group or be granted access to resources in any trusted domain. These qualities make the group type seem ideal: no worrying about whether the source of members is all right or whether the group can be assigned access in another domain.

There is a cost to this universality, however: The list of members of a universal group is kept in the Global Catalog (GC) and therefore is replicated to all domain controllers designated as Global Catalog servers in the forest. However, the new link-value replication feature in Windows Server 2003 reduces the amount of replication traffic significantly, compared to Windows 2000, where the entire universal group membership list was replicated whenever a change was made.

NOTE

Global Catalog The Global Catalog of a forest is a directory that contains a subset of each of the objects in every domain of the forest, though only some of the properties of each object. Although the main purpose of the Global Catalog is to provide an index for forestwide searches, it is also used during authentication (the process of ensuring that an object has the right to access the resources it is requesting) to get the list of all the groups a user object is a member of.

You create a universal group when both these conditions apply:

- ▶ The members of the group come from more than one domain.
- ▶ The group needs resource access in more than one domain.

Universal groups are useful when users and resources are disbursed in all domains. For example, when every domain has EngRes and Engineer Global groups, this might not be bad during the initial setup, but it becomes a nightmare as new domains are added. The Universal groups make it easier, in that each domain's Engineers Global group gets added to the Engineers Universal group, and the Engineers Universal group is added to each domain's EngRes domain local group. As new domains come online, they only have to add their Engineers Global group to the Engineers Universal group, and the Engineers Universal group to the domain local group that they have assigned permissions for the shared resources to.

Recommended Sequence of Groups

The recommended usage of groups is as follows:

- ▶ Make accounts members of global groups.
- ▶ Make global groups members of domain local groups.
- ▶ Assign resource access permissions to the domain local groups.

In some cases it is helpful to make global groups members of universal groups and then to make the universal groups members of domain local groups. This is necessary only when a universal group is needed—that is, when a group will have members from multiple domains and will need access to resources in multiple domains.

This sequence is known as *AGUDLP*, which stands for Accounts, Global, Universal, domain local, and Permissions. This is the sequence that you will use when you have multiple domains or are planning to have multiple domains in the future. If you are going to have only a single domain, the recommended sequence is *AGDLP*, which stands for Accounts, Global, Domain Local, and Permissions.

Here's the hierarchy, then: Suppose we have three domains (Trainers, Writers, and Consultants), and there is a global group in each domain that holds all the finance managers in

that domain (Trainers/G-FinanceManagers, Writers/G-FinanceManagers, and Consultants/G-FinanceManagers). We could make the U-FinanceManagers universal group with these three global groups as members, and then place the universal group on the member list of a domain local group in each of the domains to give the finance managers access to the resources the domain local group provides. Finally, we could add U-FinanceManagers to the member list of the DL-FinanceResources domain local group in each domain.

You might wonder why we don't grant access to the resources directly to the universal group. We could, of course, but our assumption is that the domain local groups would exist already, to give access to the resource to groups within the local domain.

This hierarchy of groups allows very simple handling of new employees. When a new finance manager joins any of the companies, the local administrator needs only to make the finance manager's user account a member of the G-FinanceManagers global group in the new user's local domain, and that user will immediately be able to access the resources needed.

Default Groups

In the previous chapter we discussed the various default users that are created on a Windows Server 2003 server. In addition to these user accounts, a number of default groups are created. There are different groups created, depending on whether the server is a member server or a domain controller.

These groups are preconfigured with a specific set of permissions that determine what access the users they contain are granted for a variety of resources.

Default Groups on Member Servers

A number of default groups are created on Windows Server 2003 member servers. They are managed via the Local users and Groups snap-in that was discussed in the previous chapter. They are listed here:

- ▶ *Administrators*—Members of this group have full control over the server. They can access all resources, create users and groups, and assign permissions for the resources to other users. If in a domain, the Domain Admins group is automatically made a member of this group, allowing all administrators in the domain full control access to this server.
- ▶ *Backup Operators*—Members of this group can perform backups and restores of the files on the server, even if they have not been specifically granted access to those files. However, they cannot change the security settings on the files.
- ▶ *DHCP Administrators*—Members of this group have full control over the DHCP service. They cannot access any resources not associated with DHCP without being granted additional rights. This group is present only if the DHCP role has been added to the server.

- ▶ *DHCP Users*—Members of this group can view the configuration of the DHCP server service. However, they cannot change the configuration. This group is present only if the DHCP role has been added to the server.
- ▶ *Guests*—Members of this group have limited access to the server. The Guest account is a member of this group.
- ▶ *HelpServicesGroup*—This group can be used to grant permissions to application support accounts. The default member of this group is the account used for the Remote Assistance feature.
- ▶ *Network Configuration Operators*—Members of this group have full control over the TCP/IP configuration.
- ▶ *Performance Monitor Users*—Members of this group can monitor the Performance Counters on the server, either locally or remotely. They cannot configure the performance counters.
- ▶ *Performance Log Users*—Members of this group can manage the configuration of the performance Counters on the server, either locally or remotely.
- ▶ *Power Users*—This group can be used to create and modify users and groups. They can also delete users and groups, but only those that they created. In addition, they can add users to the Power Users, Users and Guests groups, but can remove only those that they have added. They can also share resources, but can manage only those that they have created.
- ▶ *Print Operators*—Members of this group can manage printers and print queues.
- ▶ *Remote Desktop Users*—Members of this group can remotely log on to the server.
- ▶ *Replicator*—Members of this group are used to logon to the replicator service. This is more of a service account and not a user account.
- ▶ *Terminal Server Users*—This group contains the accounts of users who are currently logged on to the server remotely via Terminal Services. The default permissions assigned to this group should be sufficient for most applications.
- ▶ *Users*—Members of this group can perform common tasks on the server. If in a domain, the Domain Users group is automatically made a member of this group, allowing all users in the domain access to this server.
- ▶ *WINS Users*—Members of this group can view the configuration of the WINS server service. However, they cannot change the configuration. This group is present only if the WINS role has been added to the server.

Default Groups in Active Directory

There are several default groups created in Windows Server 2003 Active Directory. Because these are domainwide groups, they are managed via the Active Directory Users and Computers MMC, in the Builtin and the Users containers. The groups are listed here:

- ▶ *Enterprise Admins*—This group is present only in the root domain in the forest. Members of this group have full control over the forest. They can access all resources, create users and groups, and assign permissions for the resources to other users. This account is added to the membership of the local Administrators group of every workstation or member server that joins any domain in the forest.
- ▶ *Schema Admins*—This group is present only in the root domain in the forest. Members of this group have full control over the Active Directory schema.
- ▶ *Domain Admins*—Members of this group have full control over the domain. They can access all resources, create users and groups, and assign permissions for the resources to other users. This account is added to the membership of the local Administrators group of every workstation or member server that joins the domain.
- ▶ *Domain Users*—This group contains every user in the domain. This account is added to the membership of the local Users group of every workstation or member server that joins the domain.
- ▶ *Domain Guests*—Members of this group have limited access to the server. The Guest account is a member of this group.
- ▶ *Domain Controllers*—This group contains the computer accounts of all domain controllers in the domain.
- ▶ *Domain Computers*—This group contains the computer accounts of all workstations and servers added to the domain.
- ▶ *DNSAdmins*—Members of this group have full control over the DNS service. They cannot access any resources not associated with DNS without being granted additional rights.
- ▶ *DNSUpdateProxy Users*—Members of this group can perform DNS updates for other clients. Typically the DHCP servers are members of this group.
- ▶ *Account Operators*—This group can be used to create, modify, and delete users, groups, and computer accounts, except for those in the domain controllers OU. They also cannot add or remove members to the Domain Admins group.
- ▶ *Backup Operators*—Members of this group can perform backups and restores of the files in the domain, even if they have not been specifically granted access to those files. However, they cannot change the security settings on the files.

- ▶ *Cert Publishers*—Members of this group have the capability to publish security certificates in Active Directory.
- ▶ *Group Policy Creators*—Members of this group can modify Group Policy.
- ▶ *HelpServicesGroup*—This group can be used to grant permissions to application support accounts. The default member of this group is the account used for the Remote Assistance feature.
- ▶ *Incoming Forest Trust Builders*—This group is present only in the root domain in the forest. Members of this group can create one-way incoming forest trusts, but only in the forest root domain.
- ▶ *Pre-Windows 2000 Compatible Access*—This group has read access to all users and groups in the domain. The Everyone group is automatically added to this group. This group is to provide backward compatibility for computers running Windows NT 4.0.
- ▶ *Print Operators*—Members of this group can manage printers and print queues.
- ▶ *RAS and IAS Servers*—Members of this group are permitted access to the remote access properties of users in the Active Directory.
- ▶ *Server Operators*—This group can be used to manage domain controllers.
- ▶ *Terminal Service License Servers*—Members of this group distribute licenses to Terminal Services users.

EXAM ALERT

Be Sure You Know What Groups Are Built in and Their Capabilities Expect to see a few questions relating to membership of the built-in groups, especially those at the domain level.

When assigning users to the default groups, make sure that you understand exactly what access they are being given. It is usually not a good idea to assign or remove specific rights to or from a default group. It is better to create a new group and add the custom rights to it.

System Groups

The last set of default groups are System Groups. System Groups are automatically created by the operating system, but unlike the other default groups, you cannot change or manage them. In most cases, the membership of a system group is changed dynamically by the operating system. They are listed here:

- ▶ *Anonymous Logon*—This group is used to represent any users or services that access a computer over the network without a username or password. Unlike in Windows NT, the Anonymous Logon group is not a member of the Everyone group.

- ▶ *Everyone*—This group is used to represent all users or services, including those from other domains. You can grant permissions to the Everyone group, but it's not a good idea for anything other than read-only, because the Anonymous Logon group can become a member of the everyone group.
- ▶ *Network*—This group is used to represent all users accessing a specific resource over the network. The user is added to this group automatically.
- ▶ *Interactive*—This group is used to represent all users logged on locally to a computer. The user is added to this group automatically.

Creating and Modifying Groups by Using the Active Directory Users and Computers Console

Objective:

Create and modify groups by using the Active Directory Users and Computers console

To create a group with Active Directory Users and Computers, first select the domain or OU where you want the group object to reside. Generally you should place the group objects inside OUs because you will most likely delegate responsibility for all the objects in an OU to a subadministrator. In our sample company, it has been agreed that any global group that has members from outside the domain will be created at the users' level. Also, global groups will be created at the level in the hierarchy above all the objects in the groups' member list. So the DL-FinanceResources domain local group is created at the users' level, as is G-FinanceManagers. The G-PhoenixEngineers group would be created at the Phoenix OU level.

In Step by Step 3.1 we'll create groups with domain local, Global, and Universal scope.

STEP BY STEP

3.1 Creating groups with domain local, global, and universal scope

1. Open Active Directory Users and Computers and select the Phoenix OU.
2. Right-click the User OU, under the Phoenix OU.
3. Select New, Group from the context menu.
4. When the dialog box opens, ensure that the domain local and Security option buttons are selected, and then type the name **DL-FinanceResources** (see Figure 3.3).

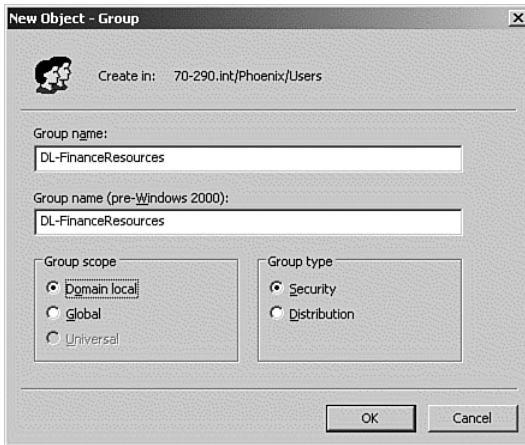


FIGURE 3.3 Give the group a name and specify its type and scope.

5. Click OK, and the group object is created.
6. Right-click the Users OU again and select New, Group from the context menu.
7. This time, ensure the Global and Security option buttons are selected, and then type the name **G-FinanceManagers** and click OK.
8. Right-click the LTI OU a third time and select New, Group from the context menu.
9. This time, ensure that the Universal and Security option buttons are selected and then type the name **U-FinanceManagers** and click OK. Now we have our three groups—and in production we would create several others (see Figure 3.4).

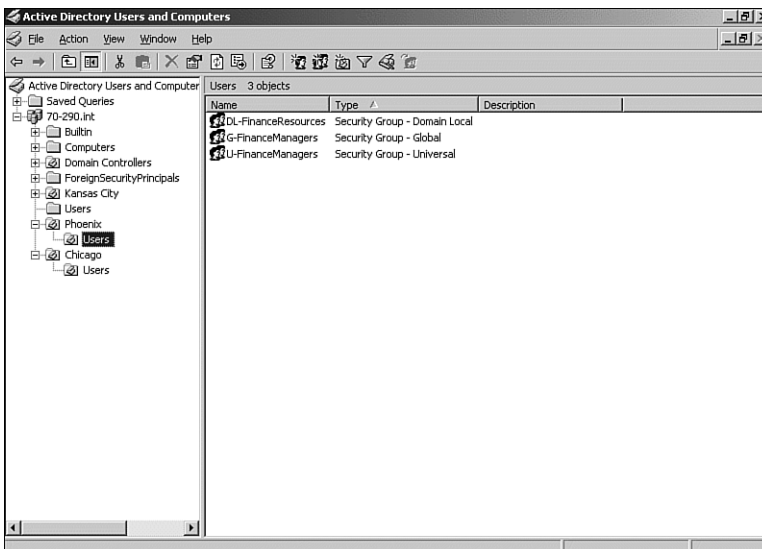


FIGURE 3.4 The group objects are shown in the details pane for the OU in which they were created.

10. Now we want to make G-FinanceManagers a member of U-FinanceManagers, and we want to make U-FinanceManagers a member of DL-FinanceResources.
11. Right-click the U-FinanceManagers object and choose Properties. Select the Members tab.
12. Click Add. In the Select Users, Contacts, Computers or Groups dialog box (in the Enter the Object Names to Select area), type **G** and click Check Names. A dialog box appears listing all the users, contacts, computers, or groups whose names start with *G* (see Figure 3.5).

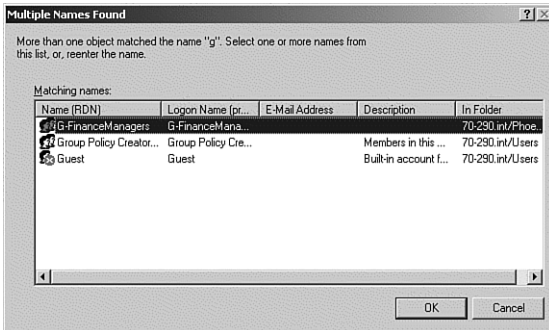


FIGURE 3.5 Select the group you want and click OK.

13. Select G-FinanceManagers and click OK twice. G-FinanceManagers is now a member of U-FinanceManagers. In production we would add the G-FinanceManagers global groups from the other domains as well.
14. Now click the Member Of tab. Select Add, type **DL** into the Enter Object Names to Select area, and click Check Names. Select DL-FinanceResources and click OK twice.
15. We now want to create the \\MARS\Finance share and give DL-FinanceResources access rights to it. To do this, start the Share a Folder Wizard by clicking Add Shared Folder from the Manage Your Server application, as shown in Figure 3.6.

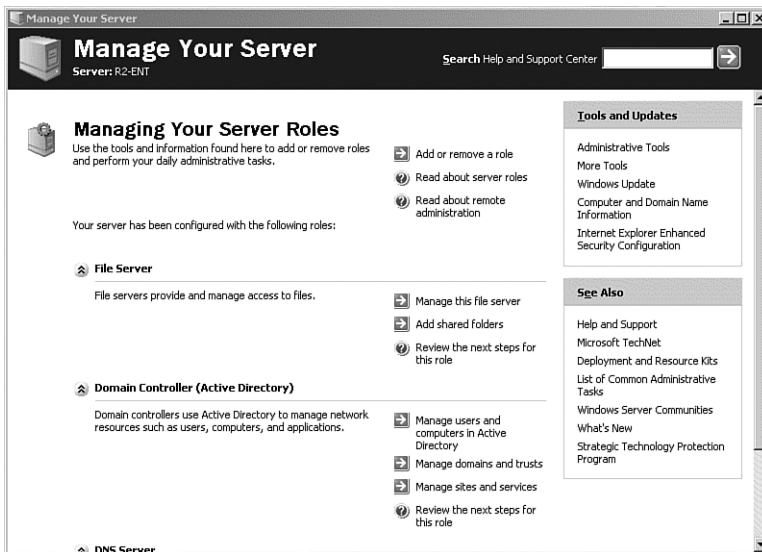


FIGURE 3.6 Select the Add Shared Folders option from the File Server category.

16. After selecting the folder to be shared, naming the share Finance, and assigning a share name, choose Use Custom Share and Folder Permissions, and in the dialog box click Add and browse to the DL-FinanceResources group. Assign the group Full Control rights, remove the Everyone group from the list, and click OK.

NOTE

Add Shared Folders The Add Shared Folders option will appear on the main screen of the Manage Your Server application only if you have added the File Server role to your server, as we did in Chapter 1, “Windows Server 2003 Environment.”

We have accomplished our task. Any member of the G-FinanceManagers global group will have the correct access to the \\MARS\Finance share.

Identifying and Modifying the Scope of a Group

Objective:

Identify and modify the scope of a group

Now you know that the scope of a group object in a domain can be domain local, Global, or Universal. (On a member server, standalone server, or workstation, local groups can also exist.) So how can you tell the scope of a group object?

The first thing to know is that it won't help you to look at the icons in the details pane of Active Directory Users and Computers. The icons used to denote group objects of all scopes are the same. However, the Type column in the details pane does indicate both the group scope and the group type. Refer to Figure 3.4 to confirm this.

Perhaps you have a global group, and you have realized that it would be useful to add accounts from another domain to the member list. That's not possible with a global group, but it is with a universal group. If you change the scope to universal, you can add members from domains in different parts of the enterprise and retain the domain local memberships the existing group has.

If the domain functionality level of your domain is Windows 2000 mixed or Windows Server 2003 interim, you cannot change a group's scope. Universal groups are not available at that domain functionality level, and you cannot change a group's scope from domain local to global, or vice versa.

If the domain functionality level is Windows 2000 native or Windows Server 2003, you can change a group's scope, but only if the group is not a member of another group and has no group members that would be illegal for groups of the new scope.

Here are some examples:

- ▶ *You want to change the scope of a group from Global to Universal*—This is not allowed if the group is a member of another global group.
- ▶ *You want to change the scope of a group from domain local to Universal*—This is not allowed if the group has another domain local group as one of its members.
- ▶ *You want to change the scope of a group from Universal to Global*—This is not allowed if the group has another universal group as one of its members.
- ▶ *You want to change the scope of a group from Universal to domain local*—This is allowed under all conditions.

NOTE

Changing Group Scope Note that it is not possible to *directly* change a domain local group to a global group, or vice versa. However, you can change a global group to a universal group and then change it to a domain local group.

To change a group's scope with Active Directory Users and Computers, first you have to select the group and look at its properties. Click the option button beside the new scope and click OK to change the scope. If you have followed group naming conventions that indicate the scope of the group, you will probably want to rename the group to show the new scope.

To determine the scope of a group object from the command line, you can use `dsget`. This command shows the description of a group, whether its type is security, and its scope:

```
dsget group <dn> [-desc] [-secgrp] [-scope]
```

To change a group's scope from the command line, you can use `dsmod`. Its syntax in this case is very simple; you just type the following:

```
dsmod group <dn> -scope <L, G, or U>
```

You must be a member of Domain Admins, Enterprise Admins, or Account Operators, or you have to have been delegated the appropriate authority to change the scope of a group by either method.

Challenge

You are a system administrator who is responsible for managing all the computer resources for your company. Your company has decided, for security reasons, to separate the Human Resources users and resources into a separate domain. However, there is a color printer in the original domain that the Human Resources department will need to use occasionally. The users in the current domain have been granted access to the printer by being members of a global group contained in a domain local group that has print permission. Both domains are running at the Windows Server 2003 functional level.

Your task is to configure the permissions for this printer so that everyone who needs access to it can print.

Try to complete this exercise on your own, listing your conclusions on a sheet of paper. After you have completed the exercise, compare your results to those given here.

1. Because there are now two separate domains, you will need to assign permissions to groups from both domains to this printer. Create a global group in the Human Resources domain who need access to this printer. Then place the Human Resources global group in the domain local group.
2. You could place all the users from both domains in a universal group and make the universal group a member of the domain local group.
3. You could create a global group in the Human Resources domain containing the users in that domain who need access to this printer. Place both global groups in a universal group, and make the universal group a member of the domain local group. This method adheres to the AGUDLP strategy.

You could also assign print permissions to a universal group and add members from both domains to it. Basically, there is no right answer to this challenge, as there are a multiple of ways to accomplish this goal.

Managing Group Membership

Objective:

Manage group membership

You can make an account a member of a group in two ways:

- ▶ Start with the properties of the account and change the list of groups of which the account is a member.
- ▶ Start with the properties of the group object and change the member list of the group.

There are several methods for changing the group membership, both from Active Directory Users and Computers and from the command line.

In Active Directory Users and Computers, you can use the Member Of tab of the account to see the list of groups the account belongs to, or you can use the Members tab of the group to see the list of members.

Let's look at the Member Of method first. Choose the properties of a user, group, or computer object in Active Directory Users and Computers, and then click the Member Of tab. A list of group objects is displayed. Click Add and use the Object Picker to locate the group or groups you want the account to be a member of. Click OK, and the Member Of list is updated, as shown in Figure 3.7.

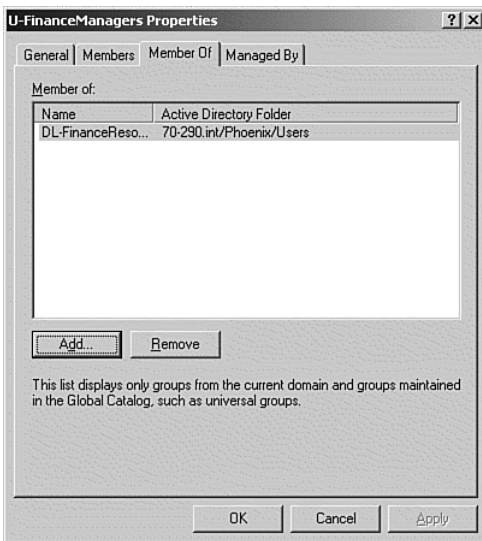


FIGURE 3.7 Click Add to make the group a member of another group.

Another way to use Active Directory Users and Computers to add accounts to a group is to select multiple accounts and then choose File, Properties, and click the Member Of tab. With the Object Picker, find the group whose member list you want to add the accounts to, select it, and select OK. Alternatively, you can right-click the objects and choose Add to a Group from the shortcut menu.

Now let's try starting from the group object. Display its properties and choose Members. Use the Object Picker again, but this time the goal is to find the accounts that should be added to the member list of the group. Select the objects and click Add.

A third method (but not recommended) is to select the accounts you want to add to a group's member list and then drag them to the group object. Dropping the accounts on the group object adds them to the member list. This method is not recommended because it is too easy to drop the accounts on the wrong group object.

There are two ways to allocate users to groups. You can either open the Membership property of a group and add users to it, or you can open the Member Of property of a user and select the groups to which that user will belong. Step by Step 3.2 shows you how to make a user a member of a group.

STEP BY STEP

3.2 Adding a member to a group

1. In Active Directory Users and Computers, navigate to a user account object and open its properties.
2. Select the Member Of tab and view the existing memberships. By default, new users created in a domain are only members of the Domain Users group, as shown in Figure 3.8.

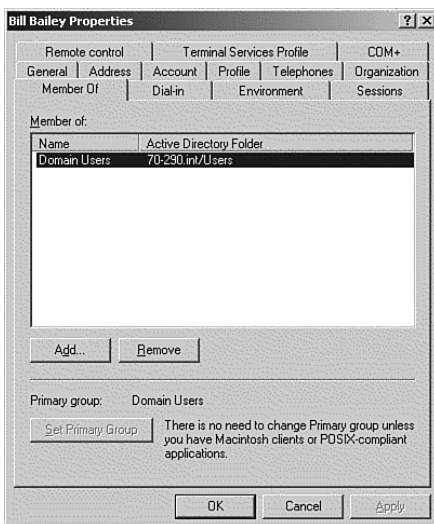


FIGURE 3.8 A new user by default is only a member of the Domain Users group.

3. Click the Add button to bring up the Select Groups dialog box. Type the name of the group and then click the Check Names button. Figure 3.9 shows the results of typing **Engineers** and then selecting Check Names.

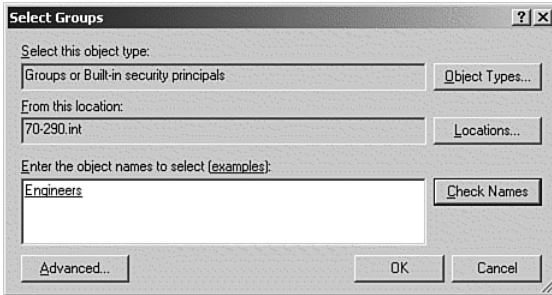


FIGURE 3.9 Adding a user to the Engineers group.

4. Click OK to complete the addition of the Engineers group to the user account and to see the new list of groups to which the user belongs.
5. Click OK to close the user's properties.

NOTE

New and Improved This is the first time we've used the new-and-improved Object Picker. In Figure 3.9, we could have typed **Eng** and clicked the Check Names button to find the Engineers group. We could have also selected the Advanced button and typed **Art** into the Name Starts With field and found both Arthur Lismer and Arthur Adams. Take a few minutes to play with the new Object Picker.

Adding Accounts to Groups with Command-Line Tools

Objective:

Create and modify groups by using automation

Naturally, a command-line tool is also available for this purpose—you can change the member list of a group with the `dsmod group` command. This command adds the accounts whose distinguished names follow `-addmbr` to the member list of the group specified:

```
dsmod group <groupdn> -addmbr <dn's of accounts to be added>
```

Note that `dsmod group` has two similar-looking parameters that can be used to alter the membership list of a group. As you can see from Table 3.2, `-chmbr` and `-addmbr` both change the membership list, but with quite different results.

TABLE 3.2 The `chmbr` and `addmbr` Commands

Parameter	Member List Before	Member List After
<code>-addmbr John</code>	Jack, Barbara, Gill, Catherine	Jack, Barbara, Gill, Catherine, John
<code>-chmbr John</code>	Jack, Barbara, Gill, Catherine	John

`dsmod` with the `-addmbr` parameter adds the account to the member list of the group, whereas the `-chmbr` parameter replaces the current member list with the accounts following `-chmbr`. And `dsmod group` with the `-rmmbr` parameter removes the accounts listed from the group's member list.

You're probably expecting to find that there is a command-line method for adding a member to a group using `dsmod user`. There isn't! In the Active Directory Users and Computers interface you cannot tell whether the group membership information is a property of the user object or the group object. But because `dsmod` allows only group membership changes with `dsmod group`, it is clear that the membership information belongs to the group object.

NOTE

Group Membership Changes As in all previous versions of the Windows server products, the group membership information is rebuilt when the user logs on. After you have changed group membership for users, be sure to tell them to log off and on again to see the effect of the group membership change.

Users on the Local Computer

Although we have been talking about domain users and domain groups in this section, you may find you need to create users and groups at the local computer level, too. Here are some examples:

- ▶ A member server in a domain may need a group account to provide access to the resources on that computer.
- ▶ You might need to share a printer installed on a standalone server, and you want to create a local group account to permit this.
- ▶ You have a computer running Windows Server 2003 that is not part of a domain, and you want to define users and groups to allow access to its resources.

These tasks are performed using Local Users and Groups in Computer Management or with the `net localgroup` command. After the users and groups have been created, you can grant them rights to access resources on the computer.

Finding Domain Groups in Which a User Is a Member

Objective:

Find domain groups in which a user is a member

If you want to know what groups a user belongs to, you can easily find out with Active Directory Users and Computers by looking at the properties of the user object and then selecting the Member Of tab. There you will see the groups the user belongs to.

There is a problem, however. What if the user is a member of group A, and group A is a member of group B? In that case, the user is effectively a member of group B, but that fact is not shown on the Member Of tab of the properties of the user object. In fact, there is no way within Active Directory Users and Computers to show the expanded member list. However, we can use `dsget user` to show this information.

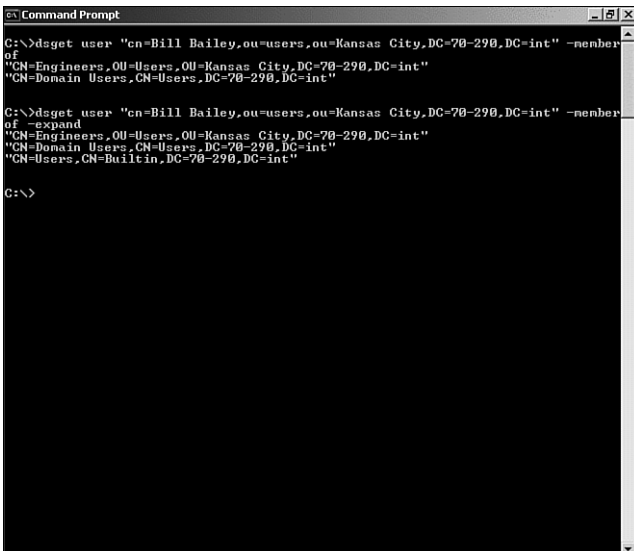
To find all the groups the user belongs to, *not counting* those due to group nesting, use the following `dsget` command:

```
dsget user <dn> -memberof
```

To find all the groups the user belongs to, including those due to group nesting, use the following `dsget` command:

```
dsget user <dn> -memberof -expand
```

In Figure 3.10, you can see the output of these two commands for the same user.



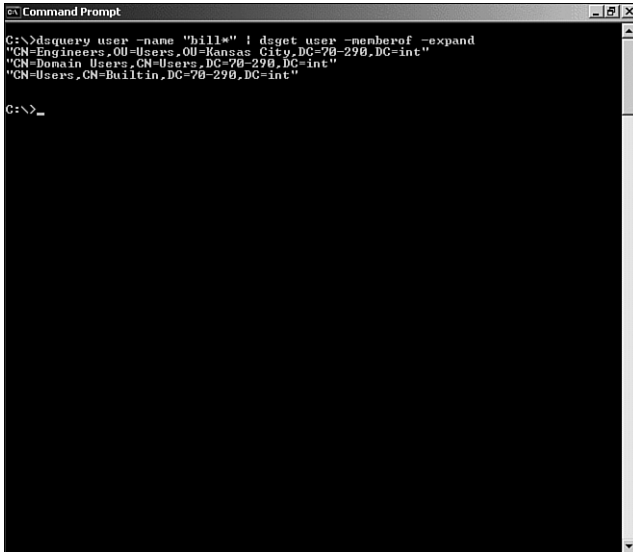
```
C:\>dsget user "cn=Bill Bailey,ou=users,ou=Kansas City,DC=70-290,DC=int" -memberof
of
"CN=Engineers,OU=Users,OU=Kansas City,DC=70-290,DC=int"
"CN=Domain Users,CN=Users,DC=70-290,DC=int"

C:\>dsget user "cn=Bill Bailey,ou=users,ou=Kansas City,DC=70-290,DC=int" -memberof -expand
of -expand
"CN=Engineers,OU=Users,OU=Kansas City,DC=70-290,DC=int"
"CN=Domain Users,CN=Users,DC=70-290,DC=int"
"CN=Users,CN=Builtin,DC=70-290,DC=int"

C:\>
```

FIGURE 3.10 The first command shows the direct group memberships of the user, whereas the second shows the nested memberships as well.

Do you remember the discussion of piping earlier in this chapter? We can pipe the output of one command to another command, which will allow us to avoid having to know the distinguished name of an account in `memberof` queries. Look at Figure 3.11.

A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt". The command entered is `C:\>dsquery user -name "bill*" | dsget user -memberof -expand`. The output consists of three lines of distinguished names: `"CN=Engineers,OU=Users,OU=Kansas City,DC=70-290,DC=int"`, `"CN=Domain Users,CN=Users,DC=70-290,DC=int"`, and `"CN=Users,CN=Builtin,DC=70-290,DC=int"`. The prompt `C:\>_` is visible at the bottom left of the window.

```
C:\>dsquery user -name "bill*" | dsget user -memberof -expand
"CN=Engineers,OU=Users,OU=Kansas City,DC=70-290,DC=int"
"CN=Domain Users,CN=Users,DC=70-290,DC=int"
"CN=Users,CN=Builtin,DC=70-290,DC=int"
C:\>_
```

FIGURE 3.11 We need to know only enough of the user's name to make the `-name` parameter unique.

As you can see from the figure, it was sufficient to enter **bill*** to select the one user whose group memberships are wanted.

Creating and Modifying Groups by Using Automation

Objective:

Create and modify groups by using automation

In Chapter 2, “Managing User and Computer Accounts,” we described using `ldifde` to create and modify user accounts. `ldifde` can also be used to create and modify group accounts.

In Step by Step 3.3, we will list the group accounts in the `KansasCity` OU, modify the names to create new group accounts, and add user accounts to the group accounts.

STEP BY STEP

3.3 Creating group accounts

1. Open a command prompt and change to the root of the C: drive.

2. Type the following command:

```
ldifde -f ldifgroupout.txt -d "OU=KansasCity,DC=70-290,
↳DC=int" -l objectclass,cn,distinguishedname,name,
↳samaccountname -r "(objectclass=group)"
```

This command will change the OU's distinguished name appropriately, if necessary, and list the group names in the `ldifgroupout.txt` file.

3. Type notepad `ldifgroupout.txt` to open the file in Notepad.

4. Change the names of the groups to new ones—for example, Marketing and Production in place of Sales and Engineering.

5. Remove the entry for `KansasCityUsers`.

6. Save the file as `ldifgroupin1.txt`.

7. Type the following command:

```
ldifde -i -f ldifgroupin1.txt -j c:\ -k
```

`-j c:\` puts a log file called `ldif.log` on `c:\`, and `-k` tells `ldifde` to continue in case of errors. You should see the message `2 entries modified successfully`.

8. In Notepad, create a file called `ldifgroupin2.txt` to change the member list of the `KansasCityUsers` group, with the following content (note that `ldifde` can replace only the complete member list of a group, so you have to include all members in this file):

```
dn: CN=KansasCity Users,OU=KansasCity,DC=70-290,DC=int
changetype: modify
replace: member
member: CN=Sales,OU=KansasCity,DC=70-290,
↳DC=intmember: CN=Engineers,OU=KansasCity,
↳DC=70-290,DC=intmember:CN=Marketing,OU=KansasCity,
↳DC=70-290,DC=int
↳member: CN=Production,OU=KansasCity,DC=70-290,DC=int
-
```

9. At the command prompt, type the following command:

```
ldifde -i -f ldifgroupin2.txt -j c:\ -k
```

You should see the message `1 entry modified successfully`.

10. In Active Directory Users and Computers, view the group objects in the `KansasCity OU` to see that the Marketing and Production groups have been created and that the four groups listed in `ldifgroupin2.txt` are shown as members of the `KansasCity OU`.

A second method of creating groups via the command line is by using the `dsadd` command. We used `dsadd` in the previous chapter to create users, and the operation is very similar.

To learn about the use of the group subcommands for `dsadd`, enter the following at the command prompt:

```
dsadd group /?
```

```
dsadd group <GroupDN> [-secgrp {yes | no}] [-scope {l | g | u}]
    [-samid <SAMName>] [-desc <Description>] [-memberof <Group ...>]
    [-members <Member ...>] [{-s <Server> | -d <Domain>}] [-u <UserName>]
    [-p {<Password> | *}] [-q] [{-uc | -uco | -uci}]
```

The `dsadd group` command can take several parameters, including group scope, group type, members, and member of, but the only required parameter is the DN (distinguished name).

For example, to create a domain local security group named DL-Engineers in the Kansas City OU, you would enter the following command:

```
Dsadd group "CN=DL-Engineers,OU=Kansas City,DC=70-290,DC=local"
    -secgrp yes -scope l
```

NOTE

dsadd For a quick review of some of the other capabilities of the `dsadd` command, refer to the section “Creating Accounts with `dsadd`” in Chapter 2.

Assigning Groups

In Windows Server 2003, you have the capability to assign a domain user as the manager of the group. This has the following advantages:

- ▶ *Assigns a contact for the group*—This gives the administrator a designated person to contact if there are any questions about the group membership.
- ▶ *Delegation*—This allows the administrator to designate a domain user to manage the additions and deletions to the group.

Delegating the management of a group allows the administrator to assign the process of maintaining the membership of a group to someone who will probably be more familiar with the changes needed to be made to the group. Usually someone like a department manager or a human resources person is responsible for managing certain groups. In Step by Step 3.4, we look at how to delegate the management of a group.

STEP BY STEP

3.4 Delegating management of a group

1. In Active Directory Users and Computers, navigate to the Users OU located under the KansasCity OU in the hierarchy.
2. In the right pane, right-click the entry for the Engineers group and select Properties.
3. Select the Managed By tab and click the Change button.
4. In the Select User, Contact or Group dialog box, enter Bill Bailey, and then click OK.
5. This returns you to the Properties dialog box as shown in Figure 3.12. Select the Manager Can Update Membership List check box.

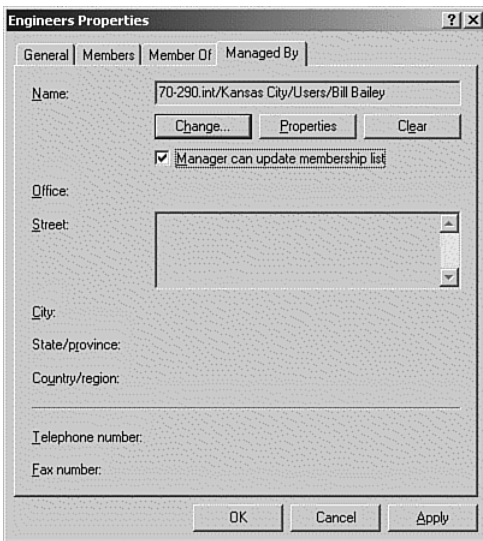


FIGURE 3.12 Grant the manager the capability to manage the membership.

6. Click OK to save.

After the administrator has created a group and assigned permissions to it, it can then be handed off to someone else to maintain the membership list. This can greatly cut down on the administrator's workload in larger companies where there are a lot of groups to maintain.

Chapter Summary

This chapter was a continuation of Chapter 2 because we discussed more of the important skills that you will use every day as a network administrator.

Here you learned about Windows Server 2003 group accounts. You discovered the two types of groups—security and distribution—and the three possible scopes a group account in a domain can have: domain local, Global, and Universal. Again, you started with Active Directory Users and Computers and progressed to the command-line tools. Then you learned about using `ldifde` to create groups.

In addition, you learned about the default groups in Windows Server 2003, and how and when they are used. Finally, you learned how to delegate some of the management of groups to an end user.

Key Terms

- ▶ AGDLP
- ▶ AGUDLP
- ▶ Domain functionality level
- ▶ Group accounts
- ▶ Group scope—domain local, Global, Universal
- ▶ Group types—distribution and security
- ▶ Nesting groups

Apply Your Knowledge

Exercises

3.1 Creating users and groups

In this exercise we will create three groups and add members to them. Then we will make the three groups members of a universal group. Because there aren't many groups to work with, we'll use Active Directory Users and Computers.

Estimated Time: 5 minutes

1. Open Active Directory Users and Computers and navigate to the LanStudents OU.

2. Create a global security group object called AdminStudents. Add the user accounts for those users whose title is Network Administrator to the member list of the group.
3. Create a global security group object called AnalystStudents. Add the user accounts for those users whose title is Systems Analyst to the member list of the group.
4. Create a global security group object called TrainerStudents. Add the user accounts for those users whose title is Trainer to the member list of the group.
5. Create a universal security group object called AllStudents. Add the three group accounts we just created to the member list of the group.

Exam Questions

1. You want to create a user account for Joan Myles using a command from the command prompt. The account is to be a member of the Engineers group in the KansasCity container, disabled when created, have Secur1ty as its password, and be placed in the "ou=Users,ou=KansasCity,DC=70-290,DC=int" container. Which of the following tools or combination of tools can do the job?
 - A. Net User followed by dsmove
 - B. Idifde followed by dsmod
 - C. dsadd
 - D. csvde followed by dsmove
 - E. dsquery followed by dsmod
2. You are the junior administrator for a large engineering firm with several locations. You read in a magazine that the best way to assign resources in a multidomain environment is to assign permissions to a domain local group, then add the Global groups to the domain local group, and then add the Global groups to a Universal group. However, the server won't let you create a Universal group. What is the most likely problem?
 - A. You don't have the proper authority.
 - B. The domain functional level is at Windows 2000 mixed.
 - C. The domain functional level is at Windows 2000 native.
 - D. The domain functional level is *not* at Windows 2003 native.

3. You are planning for resource access in a multidomain forest. Some users from all domains will need access to three continental headquarters domains. What is the recommended strategy for providing access to these resources?
- A. Users→universal groups→global groups→domain local groups→permissions to resources
 - B. Users→global groups→universal groups→domain local groups→permissions to resources
 - C. Users→domain local groups→universal groups→global groups→permissions to resources
 - D. Users→universal groups→permissions to resources
4. You are the network administrator for JJamis Inc. The network consists of a single Active Directory domain named jjamis.com. The functional level of the domain is Windows 2000 native. Some network servers run Windows 2000 Server, and others run Windows Server 2003. All users in your accounting department are members of an existing global distribution group named G-Acct. You create a new network share for the accounting users. You need to enable the members of G-Acct to access the file share. What should you do?
- A. Raise the functional level of the domain to Windows Server 2003.
 - B. Change the group type of G-Acct to security.
 - C. Change the group scope of G-Acct to universal.
 - D. Raise the functional level of the forest to Windows Server 2003.
5. You are the network administrator for JJamis Inc. The network consists of two Active Directory domains. The functional level of both of the domains is Windows 2000 mixed. Some domain controllers run Windows 2000 Server, and others run Windows Server 2003. You are trying to create a Universal group to allow you to share a printer between the two domains, but when you try to create a group, the option to create it as a Universal group is grayed out. What should you do?
- A. Raise the functional level of the domain to Windows Server 2003.
 - B. Assign permissions for the printer to a domain local group. Create a global group in each domain. Add the desired users to the global group in each domain. Add both global groups to the domain local group.
 - C. Create a global group in each domain. Add the desired users to the global group in each domain. Assign permissions for the printer to a global group. Add both user global groups to the printer global group.
 - D. Raise the functional level of the forest to Windows Server 2003.

6. You are the network administrator for JJamis Inc. The network consists of a single Active Directory domain named jjamis.com. The functional level of the domain is Windows 2000 mixed. Some domain controllers run Windows 2000 Server, and others run Windows Server 2003. All users in your accounting department are members of an existing global distribution group named G-Acct. You create a new network share for the accounting users. You need to enable the members of G-Acct to access the file share. What should you do?
- A. Raise the functional level of the domain to Windows Server 2003.
 - B. Change the group type of G-Acct to security.
 - C. Change the group type of G-Acct to universal.
 - D. Raise the functional level of the forest to Windows Server 2003.
 - E. None of the above.
7. You are the network administrator for LS Inc. The network consists of a single Active Directory domain named lsinc.com. The functional level of the domain is Windows 2000 native. You're getting ready to go to an offsite meeting, but you need to create 20 accounts for new users that are starting tomorrow morning. Your secretary is willing to enter the new accounts for you, but she has only domain user access. What should you do? Choose the best answer.
- A. Add her to the Domain Administrators group and have her create the user accounts.
 - B. Add her to the Domain Admins group and have her create the user accounts.
 - C. Add her to the Account Operators group and have her create the user accounts.
 - D. Add her to the Power Users group and have her create the user accounts.
8. You are the network administrator for LS Inc. The network consists of a single Active Directory domain named lsinc.com. The functional level of the domain is Windows 2000 native. You're in an offsite meeting, and you get a call from your secretary. The new system administrator started today. She created his account, he can log on, but he still can't access some domain resources. You gave her the permissions listed in the last question, and she successfully created his account. What is the problem? Choose the best answer.
- A. Have her add his account to the Domain Administrators group.
 - B. Have her add his account to the Domain Admins group.
 - C. Have her add his account to the Account Operators group.
 - D. Have her add his account to the Power Users group.
 - E. None of the above.

Answers to Exam Questions

- 1. B, C.** `ldifde` (with the appropriate data file as input) followed by `dsmod` (to change the password) does the job, as does `dsadd` by itself. `Net User` cannot create a group membership. `csvde` cannot create group memberships, and `dsmove` is unnecessary because `csvde` can create the user account in any container. `dsquery` cannot create a user account. See “Adding Accounts to Groups with Command-Line Tools.”
- 2. B.** Universal groups are available only at the Windows 2000 native and Windows Server 2003 functional levels. The Windows 2000 mixed and Windows Server 2003 interim levels are used to support Windows NT 4.0 domain controllers, so Global group nesting and Universal groups cannot be used. See “The Four Domain Functional Levels.”
- 3. B.** This is the recommended method for providing access to resources through group membership. See “Recommended Sequence of Groups.”
- 4. B.** Changing the group type to security is the only correct answer. Distribution groups cannot be used to assign permissions. Because this is a single domain environment, a universal group is not necessary. Changing the functional level by itself will not accomplish anything. See “Group Type.”
- 5. B.** The only correct answer is B. You can’t nest global groups in Windows 2000 mixed mode. You still have Windows 2000 domain controllers, so you can’t enable either Windows Server 2003 domain or Windows Server 2003 Forest functional levels. See “The Four Domain Functional Levels,” “The Three Forest Functional Levels,” and “Group Scope.”
- 6. E.** Distribution groups cannot be used to assign permissions. Unfortunately in Windows 2000 Mixed mode, you cannot convert a distribution group to a security group of any kind, domain local, global or universal. Because we still have Windows 2000 domain controllers, we can’t change the forest or the domain functional level to Windows Server 2003. The only solution would be to change the domain functional level to Windows 2000 native, but because it’s not listed, there is no good answer listed. See “The Four Domain Functional Levels,” “The Three Forest Functional Levels,” and “Group Scope.”
- 7. C.** There is not a Domain Administrators group, and the Power Users group is a local group. Adding a user to the Domain Admins group, even temporarily, is not a good idea because it gives them access to everything in the domain. The Account Operators group will allow your secretary to create and edit accounts without opening up too many resources on your domain. See “Default Groups.”

8. E. There is not a Domain Administrators group, and the Power Users group is a local group. It is assumed from the previous question that the secretary was added to the Account Operators group. The Account Operators group cannot add or remove users from the Domain Admins group, so the only relevant answer is E. See “Default Groups.”

Suggested Readings and Resources

1. Boswell, William. *Inside Windows Server 2003*. New Riders, 2003. ISBN 0735711585.
2. For information about LDAP, see RFCs 2251–2256. For information on LDIF, see RFC 2849.
3. Matthews, Marty. *Windows Server 2003: A Beginners Guide*. McGraw-Hill, 2003. ISBN 0072193093.
4. Minasi, Mark, et al. *Mark Minasi's Windows XP and Server 2003 Resource Kit*. Sybex, 2003. ISBN 0782140807.
5. Minasi, Mark, et al. *Mastering Windows Server 2003*. Sybex, 2003. ISBN 0782141307.
6. Shapiro, Jeffrey, et al. *Windows Server 2003 Bible*. John Wiley & Sons, 2006. ISBN 0764549375.
7. Windows Server 2003 Deployment Guide. Microsoft Corporation.
8. Windows Server 2003 Resource Kit. Microsoft Corporation.