Types of Groups

When dealing with groups, you should make the distinction between local security principals and domain security principals:

Local Users and Groups You use *local users and groups* to assign the permissions necessary to access the local machine. For example, you may assign the permissions you need to reboot a domain controller to a specific domain local group.

Domain Users and Groups *Domain users and groups*, on the other hand, are used throughout the domain. These objects are available on any of the computers within the Active Directory domain and between domains that have a trust relationship.

Here are the two main types of groups used in Active Directory:

Security Groups *Security groups* are considered security principals. They can contain user accounts, computers, or groups. To make administration simpler, system administrators usually grant permissions to groups. This allows you to change permissions easily at the Active Directory

level (instead of at the level of the resource on which the permissions are assigned).

You can also place Active Directory Contact objects within security groups, but security permissions will not apply to them.

Distribution Groups Distribution groups are not considered security principals because they do not have SIDs. As mentioned earlier, they are used only for the purpose of sending email messages.

You can add users to distribution groups just as you would add them to security groups. You can also place distribution groups within OUs so that they are easier to manage. You will find them useful, for example, if you need to send email messages to an entire department or business unit within Active Directory.

Understanding the differences between security and distribution groups is important in an Active Directory environment. For the most part, system administrators use security groups for daily administration of permissions. On the other hand, system administrators who are responsible for maintaining email distribution lists generally use distribution groups to group members of departments and business units logically. (A system administrator can

also email all of the users within a security group, but to do so, they would have to specify the email addresses for the accounts.)

When you are working in Windows Server 2003, Server 2008, Server 2008 R2, or Server 2012 functional-level domains, you can convert security groups to or from distribution groups. When group types are running in a Windows 2000 mixed domain functional level, you cannot change them.

It is vital that you understand group types when you are getting ready to take the Microsoft exams. Microsoft likes to include trick questions about putting permissions on distribution groups. Remember, only security groups can have permissions assigned to them.

Group Scope

In addition to being classified by type, each group is given a specific scope. The scope of a group defines two characteristics. First, it determines the level of security that applies to a group. Second, it

determines which users can be added to the group. *Group scope* is an important concept in network environments because it ultimately defines which resources users are able to access.

The three types of group scope are as follows:

Domain Local The scope of *domain local groups* extends as far as the local domain. When you're using the Active Directory Users and Computers tool, domain local accounts apply to the computer for which you are viewing information. Domain local groups are used to assign permissions to local resources, such as files and printers. They can contain domain locals, global groups, universal groups, and user accounts.

Global The scope of *global groups* is limited to a single domain. Global groups may contain any of the users that are a part of the Active Directory domain in which the global groups reside or other global groups. Global groups are often used for managing domain security permissions based on job functions. For example, if you need to specify permissions for the Engineering department,

you could create one or more global groups (such as EngineeringManagers and EngineeringDevelopers). You could then assign security permissions to each group.

Universal *Universal groups* can contain accounts or other universal groups from any domains within an Active Directory forest. Therefore, system administrators use them to manage security across domains. When you are managing multiple domains, it often helps to group global groups within universal groups. For instance, if you have an Engineering global group in the research.stellacon.com domain and an Engineering global group in the asia.stellacon.com domain, you can create a universal AllEngineers group that contains both of the global groups.

Now whenever you must assign security permissions to all engineers within the organization, you need only assign permissions to the AllEngineers universal group.

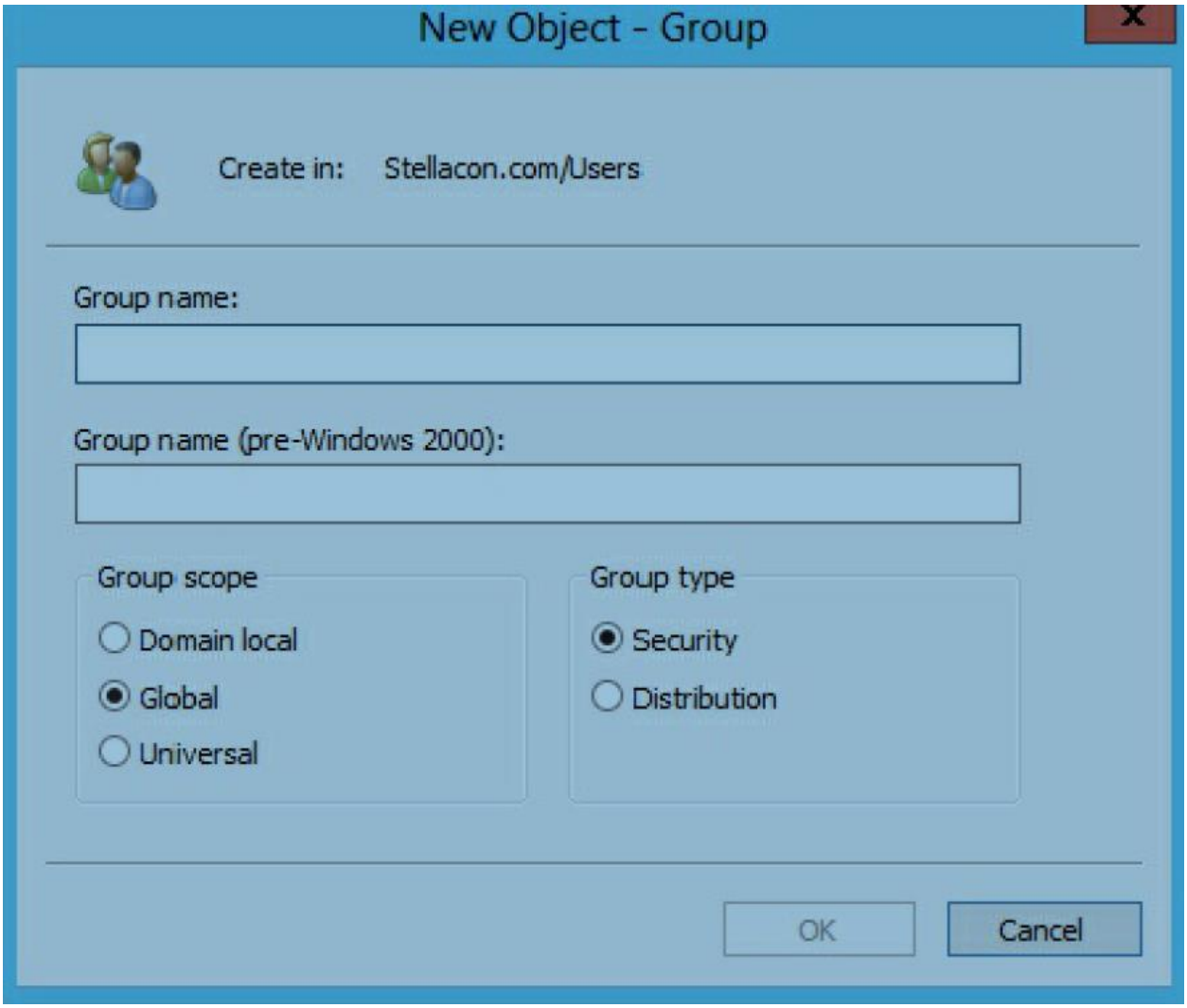
For domain controllers to process authentication between domains, information about the membership of universal groups is stored in the global catalog (GC). Keep this in mind if you ever plan to place users directly into universal groups and bypass global groups because all of

the users will be enumerated in the GC, which will impact size and performance.

Fortunately, universal group credentials are cached on domain controllers that universal group members use to log on. This process is called *universal group membership caching*. The domain controller obtains the cached data whenever universal group members log on, and then it is retained on the domain controller for 8 hours by default. This is especially useful for smaller locations, such as branch offices, that run less-expensive domain controllers. Most domain controllers at these locations cannot store a copy of the entire GC, and frequent calls to the nearest GC would require an inordinate amount of network traffic.

When you create a new group using the Active Directory Users and Computers tool, you must specify the scope of the group. Figure 13.1 shows the New Object – Group dialog box and the available options for the group scope.

FIGURE 13.1 The New Object – Group dialog box


New Object - Group
Create in: Stellacon.com/Users
Group name:
Group name (pre-Windows 2000):
Group scope
Domain local
Global
Universal
Group type
Security
Distribution
OK
Cancel