

Networking Basics: Part 14 - Security Groups

In the previous article, I showed you how to create security groups in Windows Server 2003. When I walked you through the process though, you might have noticed that Windows allows you to create a few different types of groups, as shown in Figure A. As you might have guessed, each of these group types has a specific purpose. In this article, I will explain what each type of group is used for.

Figure A: Windows allows you to create a few different types of groups

If you look at the dialog box shown above, you will notice that the Group Scope area provides you with the option of creating a domain local, global, or universal group. There is also a fourth type of group that is not shown here, it is simply called a local group.

Local groups are groups that are specific to individual computer. As you know by now, local computers can contain user accounts that are completely separate from those accounts that belong to the domain that the computer is connected to. These are known as a local user accounts, and they are only accessible from the computer on which they reside. Furthermore, local user accounts can only exist on workstations and on member servers. Domain controllers do not allow for the existence of local user accounts.

With this in mind that should come as no surprise that local groups are simply groups that are specific to a particular member server or workstation. A local group is often used to manage local user accounts. For example, the local Administrators group allows you to designate which users are administrators over the local machine.

Although a local group can only be used to secure resources residing on the local machine, it doesn't mean that the group's membership must be limited to local users. While a local group can, and usually does, contain local users, it can also contain domain users. Furthermore, local groups can also contain other groups that reside at the domain level. For example, you could make a universal group a member of a local group, and the universal group's members will basically become members of the local group. In fact, a local group can contain local users, domain users, domain local groups, global groups, and universal groups.

There are two caveats that you need to be aware of though. First, as you might have noticed, a local group cannot contain another local group. It would seem that you should be able to drop one group into another, but you can't. Someone at Microsoft once told me that the reason for this is to prevent a situation in which two local groups become members of each other.

The other caveat that you need to be aware of is that local groups can only contain domain users and domain level groups if the machine containing the local group is a member of the domain. Otherwise, local groups can only contain local users.

Given what you've just learned about local groups, the idea of a domain local group probably sounds contradictory. The reason why domain local groups exist though, is because domain controllers do not contain a local account database. This means that there are no such things as local users or local groups on a domain controller. Even so, domain controllers have local resources that need to be managed. This is where domain local groups come into play.

When you install Windows Server 2003 onto a computer, the machine typically begins life as either a standalone server or as a member server. In either case, local user accounts and local groups are created during the installation process. Now suppose that you wanted to convert the machine into a domain controller. When you run DCPROMO, the local groups and local user accounts are converted into domain local groups and domain user accounts.

It is important to keep in mind that all of the domain controllers within a domain share a common user account database. This means that if you add a user to a domain local group on one domain controller, the user will be a member of that domain local group on every domain controller in the entire domain.

The most important thing to keep in mind about domain local groups is that there are two different types. As I mentioned, when DCPROMO is run, the local groups are converted to domain local groups. Any domain local groups that are created by running DCPROMO are placed into the Builtin folder in the Active Directory Users and Computers console, as shown in Figure B.

Figure B: Domain local groups created by DCPROMO reside in the Builtin container

The reason why this is important to know is because there are some restrictions imposed on these particular domain local groups. These groups cannot be moved or deleted. Likewise, if you cannot make these groups members of other

domain local groups.

These restrictions do not apply to domain local groups that you create though. Domain local groups that you create typically began life in the Users container. From there, you are free to move or delete them to your heart's content.

I have to be perfectly frank and tell you though that in all the years I have been working with Windows Server, I have yet to find a good argument for creating domain local groups. In fact, domain local groups are basically identical to global groups, except that they are restricted to an individual domain.

Global groups are by far the most commonly used type of group. In most cases, a global group simply acts as a collection of Active Directory user accounts. The interesting thing about global groups is that they can be placed inside of each other. You can make one global group a member of another global group, so long as both global groups exist within the same domain.

Keep in mind, the global groups can only contain Active Directory resource. You cannot place a local user account or a local group into a global group. You can however, add a global group to a local group. In fact, doing so is the most common way of granting domain users permissions to resources stored on a local computer. For example, suppose that you wanted to give the managers in your company administrative rights to their workstations (not that I recommend doing that, this is just an example). To do so, you could create a global group called Managers, and place each of the manager's domain user accounts into it. You could then add the Managers group to the workstation's local Administrators group, thus making the managers administrators on those workstations.

In this article, I've explained that Windows supports the use of four different types of security groups. So far, I have explained the differences between local, domain local, and global groups. In the next part of this article series, I will continue the discussion by discussing universal groups. I will then go on to discuss the concept of group nesting