Group Scope in Active Directory

blog.netwrix.com/2022/10/19/group-scope-in-active-directory

Joe Dibley

IT pros are well aware that Active Directory has two types of groups: **security groups**, which are used to assign permissions to shared resources, and **distribution groups**, which are used to create email distribution lists. But not everyone understands that each of these Active Directory groups has a **scope** — and understanding how scope works is vital to security and business continuity. This blog post dives into what group scope is and exactly why it's important. We'll also present Microsoft's best practice models for using group scope in Active Directory, including the key positives and negatives of each.

Handpicked related content:

[Free Guide] Active Directory Group Management Best Practices

What is group scope?

The scope of an AD group determines both where the group can be applied in the forest or domain and who can be a member of a group. Because Active Directory has few limitations on how groups can be nested within each other, group nesting can present massive security and operational risks to an organization. The only real help that AD offers to combat the risks of nesting security groups is group scope.

What types of group scope are there?

There are three group scopes: universal, global and domain local. The table below was taken straight from Microsoft TechNet and it gives the whole story of the rules for group scope:

Group Scope	Group can include as members…	Group can be assigned permissions in…	Group scope can be converted to…
Universal	• Accounts from any domain within the forest in which the universal group resides • Global groups from any domain within the forest in which the universal group resides • Universal groups from any domain within the forest in which the universal group resides	Any domain or forest	• Domain local • Global (as long as no other universal groups exist as members)
Global	• Accounts from the same domain as the parent global group • Global groups from the same domain as the parent global group	Member permissions can be assigned in any domain	Universal (as long as it is not a member of any other global groups)
Domain local	• Accounts from any domain • Global groups from any domain • Universal groups from any domain • Domain local groups but only from the same domain as the parent domain local group	Member permissions can be assigned only within the same domain as the parent domain local group	Universal (as long as no other domain local groups exist as members)

Group scope and AD security models

The goal of a well-architected AD is to provide each user with exactly the right level of access to data and resources that they need to do their job. Microsoft defines two best-practice models for AD architecture:

- AGDLP (account, global and domain local permission)
- AGUDLP (account, global, universal and domain local permission)

The AGDLP model

The AGDLP model provides a guide for how to nest groups without compromising Active Directory security or sacrificing operational efficiency: User and computer accounts should be members of global groups, which are in turn members of domain local groups that describe resource permissions.

The rationale behind this can be a little tricky, but we'll do our best to break it down here. Think of global groups as "account groups" — they are used to contain user and computer accounts (as well as other global groups), all from the same domain. A group cannot contain users or computers from other domains. The users typically are in the same department, have the same manager or exhibit some other similarity. For instance, everyone in the Marketing department of the New York headquarters of a company would be put into the same global group called "New York Marketing".

Domain local groups are "resource groups" because the greater flexibility in their membership makes local domain groups ideal for granting permissions on resources. In particular, domain local groups can include members not just from the parent domain but from other domains and trusted forests. This enables administrators to grant access to a resource to anyone in the environment who needs it. To continue our example, we might define a domain local group that grants access to a file share called "Marketing Documents". By nesting the "New York Marketing" global group inside the "Marketing Documents" domain local group, we give everyone in the New York Marketing team access to the contents of the Marketing Documents share.

Here is a graphical representation of this AGDLP scenario:

All About AGDLP Group Scope for Active Directory

The use of domain local groups becomes especially important when you are dealing have trusted forests. In those cases, chances are good that accounts in one forest will need access to resources in the other forest. If a global group was used to grant access to a resource, there would be no way for accounts in the other forest to be given access to that resource, since accounts and groups cannot be nested into global groups from a different domain or forest.

To continue with our example, perhaps our company acquires a firm in Miami and the IT groups decide to establish trusts between the two companies' forests. Under the AGDLP model, the Miami-based company's forest includes a global group for their Marketing department, called "Miami Marketing". In order to give those team members access to the Marketing Documents share, all the admin has to do is nest the Miami Marketing global group in the Marketing Documents domain local group, as illustrated below:

All About AGDLP Group Scope for Active Directory 2

The AGUDLP model

The AGUDLP model is very similar to AGDLP but introduces the universal groups into the equation (hence the “U” in its name). The memberships of these groups are stored in the global catalog, which is more of a necessity in multi-domain environments. The use of this model really depends on how much the global catalog is relied on in the organization. If there is a vested interest in having the global catalog be as complete as possible (perhaps you have a large mobile workforce and rely heavily on employees being able to easily find each other in Outlook), then the AGUDLP model will help in this endeavor. However, for smaller environments that have only a single domain, this model may add an unnecessary layer of complexity.

The benefits of these models

The reason these models are Microsoft best practices is two-fold. First, there is the security perspective: If admins were to use global groups to give users permissions to resources, they would have to add users from other domains and forests into the domain where the resources reside. Generally, separate domains and forests exist for a reason and the delineations between domains and forests are not meant to be blurred. By using domain local groups to grant permissions to specific resources, an admin can give members from other domains and forests access to the resource without needing to give them direct access to the rest of the domain where that resource lives. All too often, we see organizations use global groups to assign permissions on resources and end up over-provisioning access and rights as a result when users move in and out of the group.

Second, from an operational perspective, the AGDLP and AGUDLP models make group membership management easier because permissions and users are managed in distinct places. Resource permissions are set for domain local groups and rarely need to change, limiting how often IT pros have to make adjustments. Users, in contrast, are constantly coming and going or moving around the organization, but all IT pros need to do to maintain proper levels of access is to update the global groups.

It should be noted that just because these models are Microsoft's best practices, they are not perfect for everyone. In larger environments, the use of domain local groups to manage resource permissions can lead a very large number of groups. This could result in a user being a member of thousands of groups to gain access to all of the resources they need, causing issues like token bloat.

Summary

At the end of the day, following the AGDLP and AGUDLP models offers very real benefits to an organization. The trouble often lies in implementation, since it requires more than just a savvy admin to shuffle groups around in AD. These models necessitate constant vigilance and oversight on the part of IT and the business, including assigning each group an owner who understand the needs of the users in the group and building a process to regularly ensure that the right users are in the right groups and that each group has the correct permissions on resources.

How Netwrix can help

The good news is that there are tools that can help with these steps. The Netwrix Active Directory Security Solution empowers organizations to quickly get on track toward effective access management by identifying the groups you have, what resources they grant access to, which users are in each group and what rights those users have. Furthermore, the solution helps identify group owners and makes it easy to give them the ability to manage their own groups, since they know better than anyone else who needs access to what. While it can be a monumental effort to adopt an AGDLP or AGUDLP model, doing so can go a long way towards ensuring a secure, sustainable environment.

FAQ

What is group scope in Active Directory?

Group scope indicates how widely the group is used in the domain or forest.

How many group scope types are there in Active Directory?

Active Directory defines the following three group scopes: universal, global and domain local.

What is the difference between global and universal group scope?

The primary difference is that global groups can contain members from the same domain only, while universal groups can contain objects from any domain in the same Windows forest. (Keep in mind that forest-wide replication is **not** triggered for changes to global group membership.)

Joe Dibley
Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.