Security Groups

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#what-is-a-security-group-in-active-directory

What is a security group in Active Directory?

Active Directory has two forms of common security principals: user accounts and computer accounts. These accounts represent a physical entity that is either a person or a computer. A user account also can be used as a dedicated service account for some applications.

Security groups are a way to collect user accounts, computer accounts, and other groups into manageable units.

In the Windows Server operating system, several built-in accounts and security groups are preconfigured with the appropriate rights and permissions to perform specific tasks. In Active Directory, administrative responsibilities are separated into two types of administrators:

- **Service administrators**: Responsible for maintaining and delivering Active Directory Domain Services (AD DS), including managing domain controllers and configuring AD DS.
- **Data administrators**: Responsible for maintaining the data that's stored in AD DS and on domain member servers and workstations.

How Active Directory security groups work

Use groups to collect user accounts, computer accounts, and other groups into manageable units. Working with groups instead of with individual users helps you simplify network maintenance and administration.

Active Directory has two types of groups:

- **Security groups**: Use to assign permissions to shared resources.
- **Distribution groups**: Use to create email distribution lists.

Security groups

Security groups can provide an efficient way to assign access to resources on your network. By using security groups, you can:

- Assign user rights to security groups in Active Directory.
  Assign user rights to a security group to determine what members of that group can do within the scope of a domain or forest. User rights are automatically assigned to some security groups when Active Directory is installed to help administrators define a person's administrative role in the domain.
  For example, a user who you add to the Backup Operators group in Active Directory can back up and restore files and directories that are located on each domain controller in the domain. The user can complete these actions because, by default, the user rights *Backup files and directories* and *Restore files and directories* are automatically assigned to the Backup Operators group. Therefore, members of this group inherit the user rights that are assigned to that group.
  You can use Group Policy to assign user rights to security groups to delegate specific tasks. For more information about using Group Policy, see User Rights Assignment.
- Assign permissions to security groups for resources.
  Permissions are different from user rights. Permissions are assigned to a security group for a shared resource. Permissions determine who can access the resource and the level of access, such as Full control or Read. Some permissions that are set on domain objects are automatically assigned to allow various levels of access to default security groups like the Account Operators group or the Domain Admins group.
  Security groups are listed in Discretionary Access Control Lists (DACLs) that define permissions on resources and objects. When administrators assign permissions for resources like file shares or printers, they should assign those permissions to a security group instead of to individual users. The permissions are assigned once to the group instead of multiple times to each individual user. Each account that's added to a group receives the rights that are assigned to that group in Active Directory. The user receives permissions that are defined for that group.

You can use a security group as an email entity. Sending an email message to a security group sends the message to all the members of the group.

Distribution groups

You can use distribution groups only to send email to collections of users by using an email application like Exchange Server. Distribution groups aren't security enabled, so you can't include them in DACLs.

Group scope

Each group has a scope that identifies the extent to which the group is applied in the domain tree or forest. The scope of a group defines where in the network permissions can be granted for the group. Active Directory defines the following three group scopes:

- Universal
- Global
- Domain Local

Note

In addition to these three scopes, the default groups in the Builtin container have a group scope of Builtin Local. This group scope and group type can't be changed.

The following table describes the three group scopes and how they work as security groups:

Expand table

Scope	Possible members	Scope conversion	Can grant permissions	Possible member of
Universal	Accounts from any domain in the same forest Global groups from any domain in the same forest Other Universal groups from any domain in the same forest	Can be converted to Domain Local scope if the group isn't a member of any other Universal group Can be converted to Global scope if the group doesn't contain any other Universal group	On any domain in the same forest or trusting forests	Other Universal groups in the same forest Domain Local groups in the same forest or trusting forests Local groups on computers in the same forest or trusting forests
Global	Accounts from the same domain Other Global groups from the same domain	Can be converted to Universal scope if the group isn't a member of any other Global group	On any domain in the same forest, or trusting domains or forests	Universal groups from any domain in the same forest Other Global groups from the same domain Domain Local groups from any domain in the same forest, or from any trusting domain

Scope	Possible members	Scope conversion	Can grant permissions	Possible member of
Domain Local	Accounts from any domain or any trusted domain Global groups from any domain or any trusted domain Universal groups from any domain in the same forest Other Domain Local groups from the same domain Accounts, Global groups, and Universal groups from other forests and from external domains	Can be converted to Universal scope if the group doesn't contain any other Domain Local group	Within the same domain	Other Domain Local groups from the same domain Local groups on computers in the same domain, excluding built-in groups that have well-known security identifiers (SIDs)

Special identity groups

Special identities are referred to as groups. Special identity groups don't have specific memberships that you can modify, but they can represent different users at different times depending on the circumstances. Some of these groups include Creator Owner, Batch, and Authenticated User.

For more information, see Special identity groups.

Default security groups

Default groups like the Domain Admins group are security groups that are created automatically when you create an Active Directory domain. You can use these predefined groups to help control access to shared resources and to delegate specific domain-wide administrative roles.

Many default groups are automatically assigned a set of user rights that authorize members of the group to perform specific actions in a domain, like logging on to a local system or backing up files and folders. For example, a member of the Backup Operators group can perform backup operations for all domain controllers in the domain.

When you add a user to a group, the user receives all the user rights that are assigned to the group, including all the permissions that are assigned to the group for any shared resources.

Default groups are located in the Builtin container and in the Users container in Active Directory Users and Computers. The Builtin container includes groups that are defined with the Domain Local scope. The Users container includes groups that are defined with Global scope and groups that are defined with Domain Local scope. You can move groups that are located in these containers to other groups or organizational units within the domain, but you can't move them to other domains.

Some of the administrative groups that are listed in this article and all members of these groups are protected by a background process that periodically checks for and applies a specific security descriptor. This descriptor is a data structure that contains security information that's associated with a protected object. This process ensures that any successful unauthorized attempt to modify the security descriptor on one of the administrative accounts or groups is overwritten with the protected settings.

The security descriptor is present on the AdminSDHolder object. If you want to modify the permissions on one of the service administrator groups or on any of its member accounts, you must modify the security descriptor on the AdminSDHolder object so that it's applied consistently. Be careful when you make these modifications because you're also changing the default settings that are applied to all your protected administrative accounts.

Revision #1
Created 30 March 2024 12:34:31 by ColtM
Updated 7 August 2024 23:24:39 by ColtM