Samba Active Directory Domain Controller Delegation

Introduction

Active Directory allows you to delegate permission for administration tasks to users and/or groups. This is an important feature that allows you to prevent working with domain admin permissions the whole time or giving the domain admin password to all in your IT department.

Possible fields of application:

- Allow supporters to join machines to the domain.
- Allow the human resources to update general user information.
- Allow the HelpDesk workers to create users, reset passwords and unlock accounts.

Delegations can be configured on the whole domain or on specific OUs.

Samba versions supporting delegations

You should at least run 4.0.0 final (older versions haven't been tested)!

Known issues/limitations

- 4.0.0 - current: Delegations working fine, but because of ACL issues, you have to add 'acl:search=false' as a workaround to your smb.conf (See https://bugzilla.samba.org/show_bug.cgi?id=9788).
- When upgrading from a version prior 4.0.5 to that version or later: If you run 'samba-tool dbcheck --reset-well-known-acls - -fix' to reset the directory ACLs (recommended in 4.0.5 release notes to fix missing ACLs from previous provisioning), you'll loose all existing delegations. But you should fix the wrong directory ACLs that where provisioned by earlier versions!

Performance and maintanance of delegations

Delegations are simply said ACLs on directory attributes and containers. If you would delegate permissions for several users accounts, this would increase the number of ACLs, what could cause performance impacts somewhen. Also if the delegated permissions should be revoked for an account,

you have to remove its ACLs, what brings unneccessary administration work.

That's why it is recommented, that you delegate permissions only to groups and not to accounts. If you want to grant/revoke permissions for an account, you only have to change the group membership.

Delegating 'Joining Computers to the domain'-permissions

Add delegation

In the following we'll explain how you delegate permission for joining computers to the domain to members of a non-domain-admin-group. This delegation should only be set on the default container for machine accounts (CN=Computers).

Side note: By default, the 'authenticated users' group can join up to 10 workstations to the domain. This can be a security risk and you should think about deactivating this!

- Open the ADUC console as domain administrator.
- Create a new group 'supporters' and add user accounts to it, who should later be able to join machines to the domain.
- Right-click to CN=Computers and click 'Delegate control' to open the delegation wizzard.
- Click 'Next'.
- Click 'Add' and add the group 'supporters'. Click 'Next'.
- Choose 'Create a custom task to delegate' on the 'Tasks to delegate' window.
- In the 'Active Directory Object Type' window, select 'Only the following objects in the folder' and check 'Computer objects' out of the list. Also check the two options 'Create selected objects in this folder' and 'Delete selected objects in this folder'. Click 'Next'.
- In the 'Permissions' window, check 'General' and 'Property-specific'. Also select the following permissions from the list:
    - Reset password.
    - Read and write account restrictions.
    - Read and write DNS host name attributes.
    - Validated write to DNS host name.
    - Validated write to service principal name.
    - Write servicePrincipalName.
- Click 'Next'.
- Click 'Finish'.

After you finished these steps, members of the 'supporter' group will be able to join computers to the domain.

Revoke delegation

If you want to revoke the permission for the 'supporter' group again, follow these steps:

- Open the ADUC console as domain administrator.
- Right-click to the container on which you want to revoke the permissions and click 'properties'.
- Go to the 'security' tab.
- Delete the 'supporter' group from the list.
- Click 'OK'.

Delegating 'Add/change/delete accounts/groups'-permissions

Usually you don't want to be logged in the whole day as Domain Administrator. But to do changes on user accounts and groups, you need special permissions in the AD. Per default, all members of the BuiltIn group “Account Operators” can do this job. So simply add the user/s who should be able do administrate accounts and groups to this group.

But the “Account Operators” group doesn't have permissions, that are required for doing all changes on the “UNIX attributes” tab. To archive this, follow these steps:

- Open the ADUC console as domain administrator.
- Right-click to the container “System” / “RpcServices” and choose “Properties”.
- Go to the “Security” tab.
- Click the “Add” button and search for the “Account Operators” group.
- Select permissions “Full control” for this group.
- Click the “Advanced” button.
- Select the “Account Operators” entry, click “Edit” and change the “Apply onto” field to “This object and all child objects” and close all windows with “OK” to save the changes.