Managing local groups on domain members via GPO restricted groups

From SambaWiki

Contents

Introduction

AD administrators often have the requirement to manage local group memberships of Windows workstations and servers from on a central way. Group Policies Restricted Groups is a simple way to accomplish this requirement and works in a Samba AD as well as in a MS controlled.

Restricted Groups are non-tatooing changes. This means, if you undo this change in the GPO, the changes are reset to their previous state on the affected computers after the next GPO refresh.

A best practice is, to use only AD groups instead of individual user accounts, to add to local groups. This allows changes on a central place (AD), by adding/removing members to/from the group, instead of modifying the GPO.

For simplicity, all examples in this documentation are configured on domain level through the Default Domain Policy. Needless to say, that is possible in self-created GPOs and OU-level, too.

Preconditions

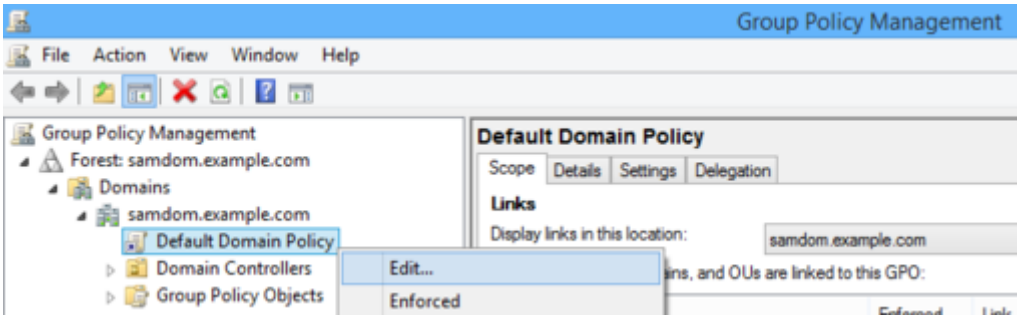
- Installed Group Policy Management Console. It is part of the Remote Server Administration Tools (RSAT).
- The examples used below add a AD domain group „SAMDOM\Wks Admins“. Groups can be added to the AD using 'samba-tool' or Active Directory User and Computer (ADUC).

Modify local group membership and keep existing members

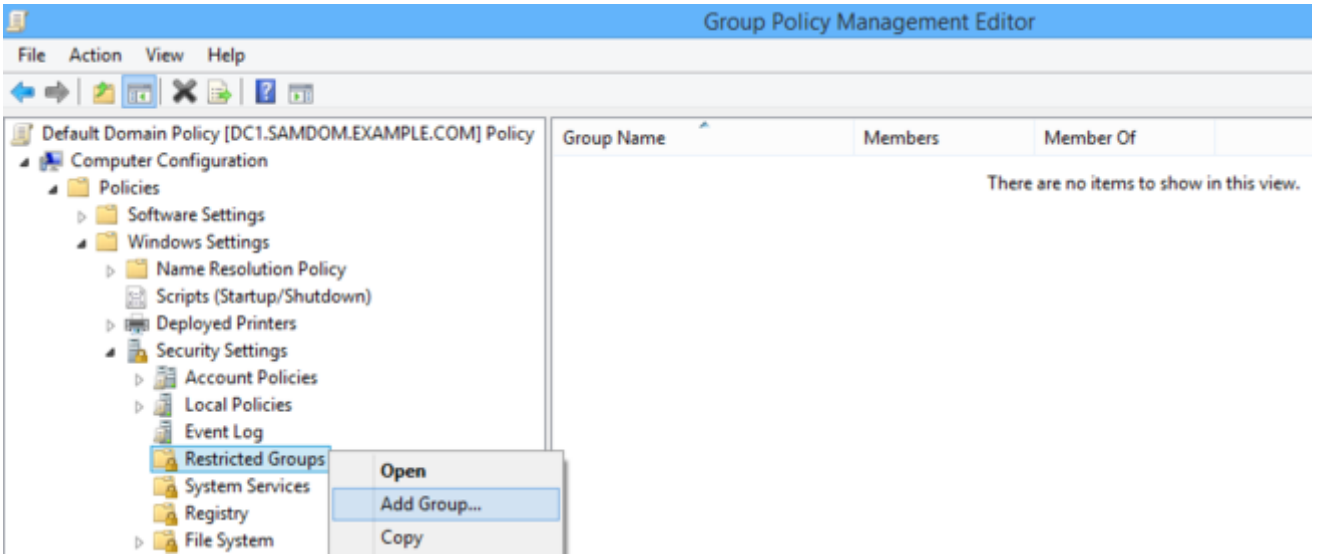
This is the most typical field of application: An AD group should be added as a member to a local group and all already existing members should be untouched.

Example: The AD domain group „SAMDOM\Wks Admins“ should be added to the local „Administrators“ group on all computers in the domain (workstations and server). The members of this domain group can be managed central in AD and allows e. g. supporter accounts to have local administrator permissions on all Windows computers, without knowing the Domain Administrator password or being member of the „Domain Admins“ group. All existing members in the local „Administrators“ group should stay. Only the domain group „SAMDOM\Wks Admins“should be added.

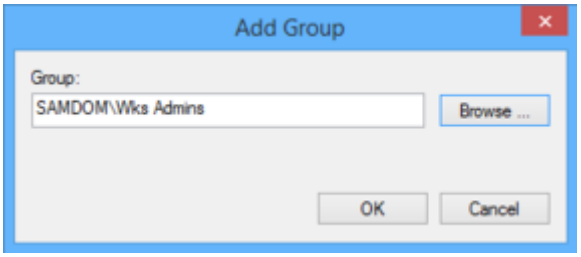
- Create a domain group „Wks Admins“, using 'samba-tool' or Active Directory Users and Computers from the Remote Server Administration Tools (RSAT).
- Open the Group Policy Management Console
- Right-click to „Default Domain Policy“ and choose „Edit...“



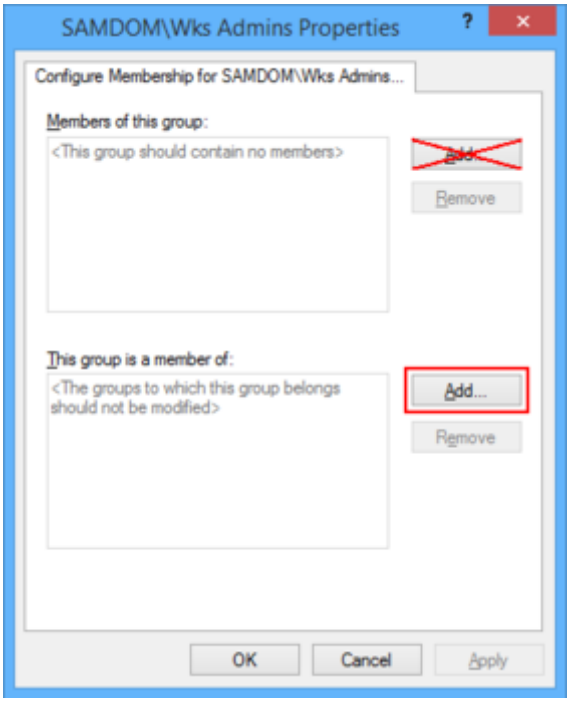
- The Group Policy Management Editor opens
- Navigate and right-click to „Computer Configuration“ / „Policies“ / „Windows Settings“ / „Security Settings“ / „Restricted Groups“ and choose „Add group...“.



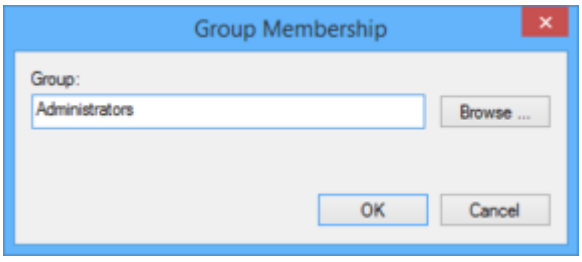
- Enter the name of the AD group „SAMDOM\Wks Admins“ by browsing your directory and click „OK“.



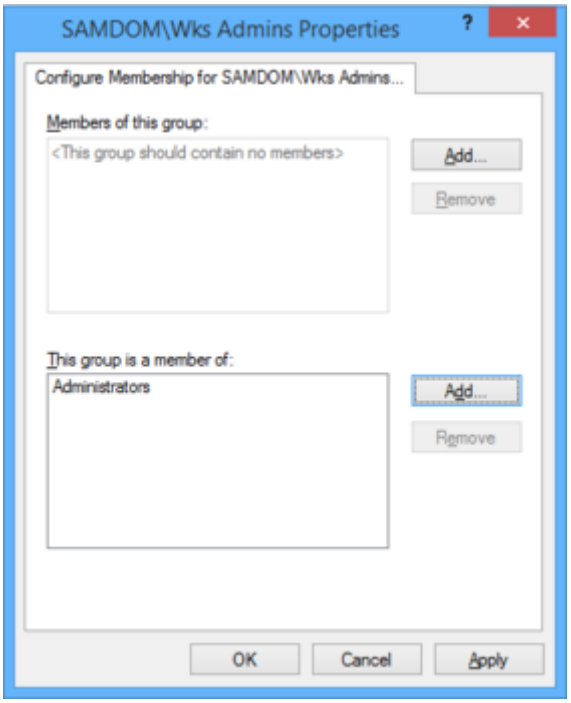
- The properties window opens. Click the „Add“ button next to the „This group is a member of“ box.



- Enter the local „Administrators“ group name. If you use the „Browse“ button, select the local computer, by using the „Locations...“ button in the upcomming window, to browse local instead of AD security objects!

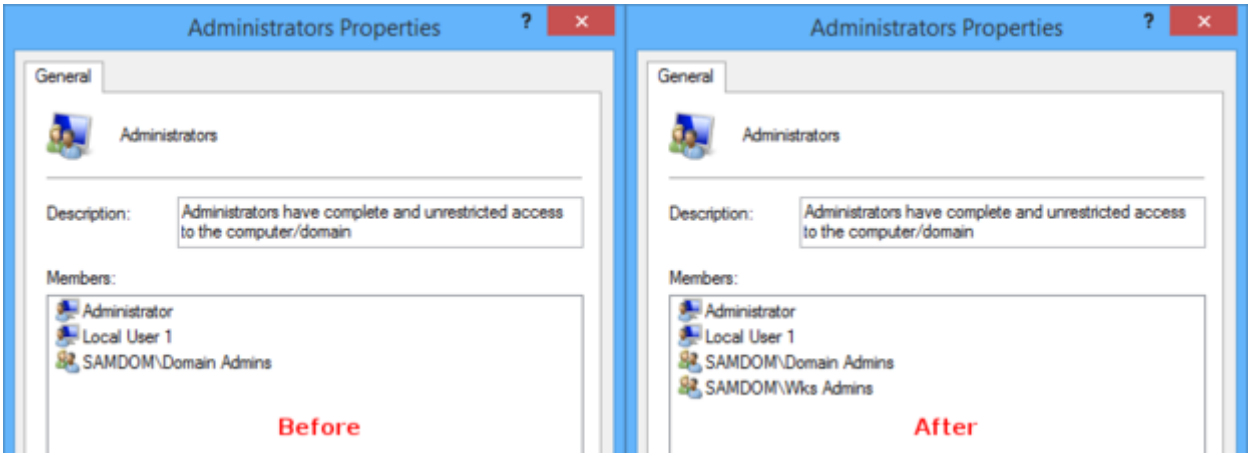


- You see the local „Administrators“ group entry in the „This group is a member of“ list.



- Click „OK“.

After the clients have re-read the changed group policy, the domain group „SAMDOM\Wks Admins“ will appear in the local „Administrators“ group on each client affected by the GPO. All existing members of this group stay untouched.



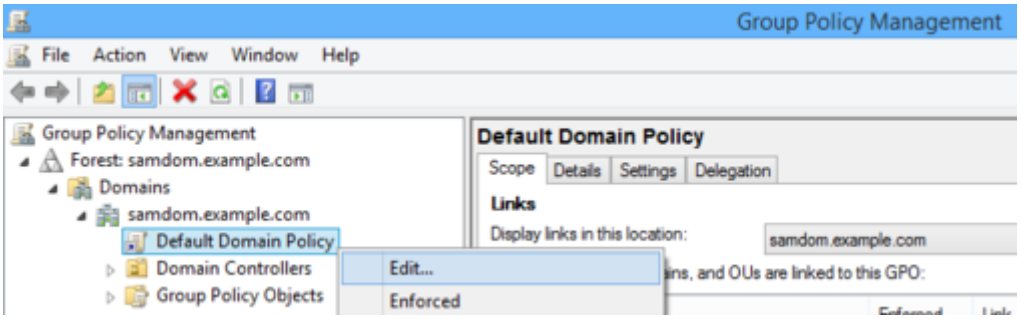
Explicit control of local group membership

This way describes how to explicitly set the membership of a local group by replacing existing memberships with the ones defined in the GPO. Use this with care, to ensure that you don't break existing permissions of accounts used by users and applications!

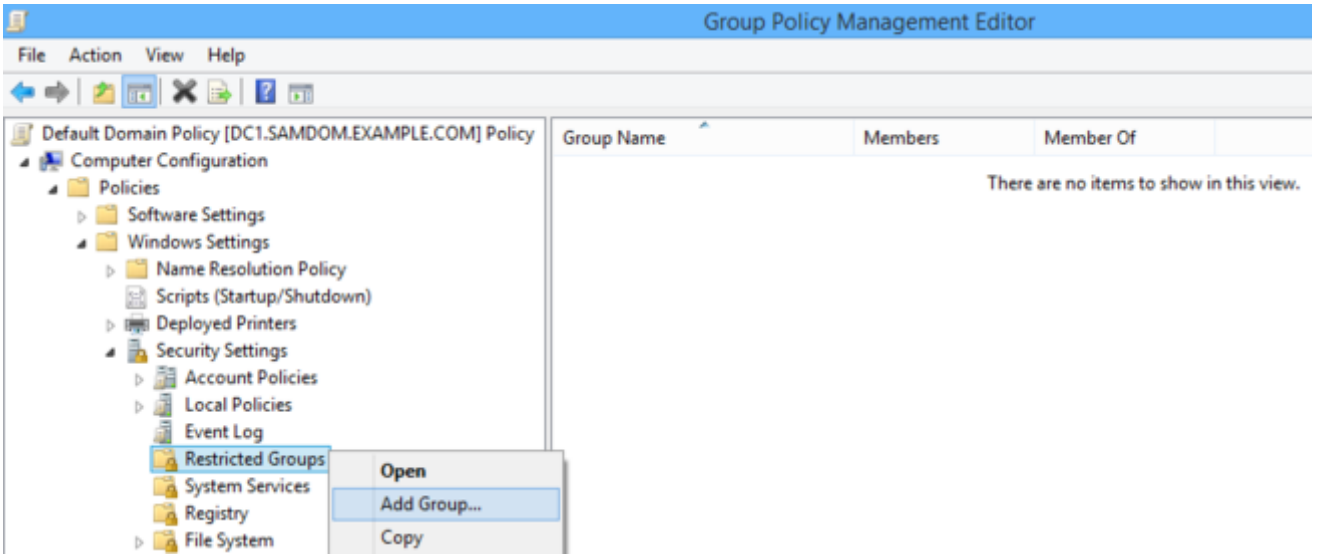
Example: On all computer in the domain (workstations and servers), the local Administrator and the domain group „SAMDOM\Wks Admins“ should be the only members of the local „Administrators“ group. All existing members of this group should be removed and just these two objects should be part of it.

- Create a domain group „Wks Admins“, using 'samba-tool' or Active Directory Users and Computers from the Remote Server Administration Tools (RSAT).

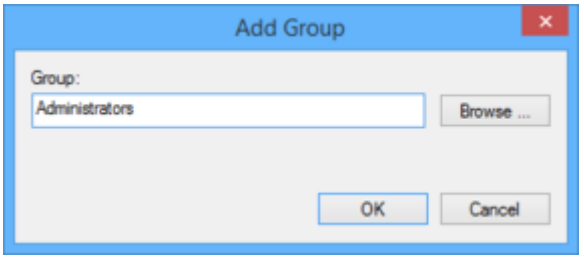
- Open the Group Policy Management Console
- Right-click to „Default Domain Policy“ and choose „Edit...“



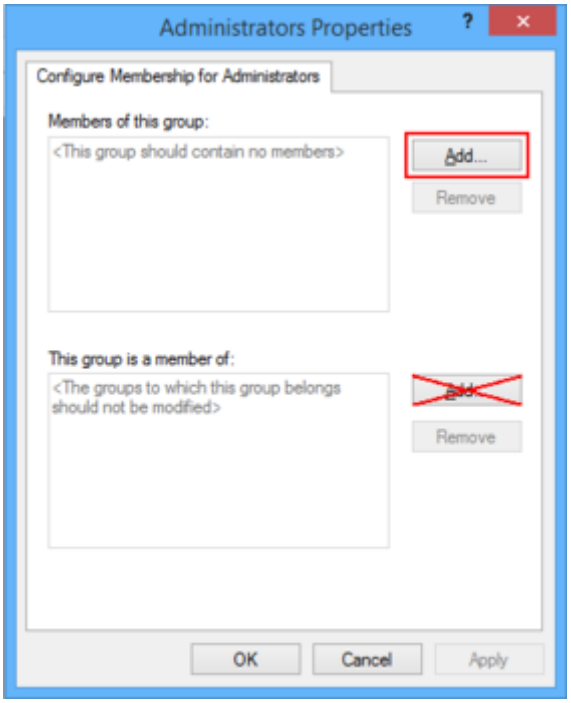
- The Group Policy Management Editor opens
- Navigate and right-click to „Computer Configuration“ / „Policies“ / „Windows Settings“ / „Security Settings“ / „Restricted Groups“ and choose „Add group...“.



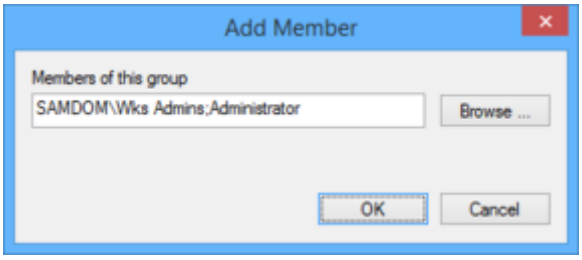
- Enter the local „Administrators“ group name. If you use the „Browse“ button, select the local computer, by using the „Locations...“ button in the upcomming window, to browse local instead of AD security objects!



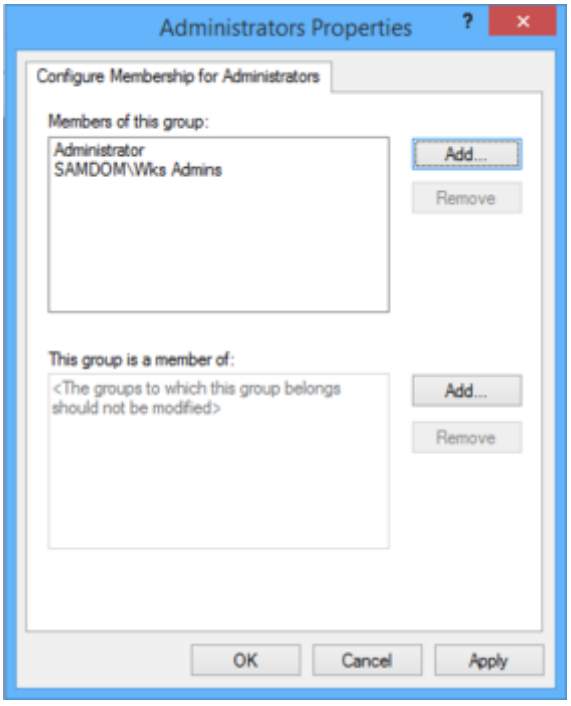
- Click the „Add“ button next to the „Members of this group“ box.



- Enter the domain group „SAMDOM\Wks Admins“ and the local „Administrator“ account. If you use the „Browse“ button, select the domain/local computer, by using the „Locations...“ button, to browse the domain/local security objects!

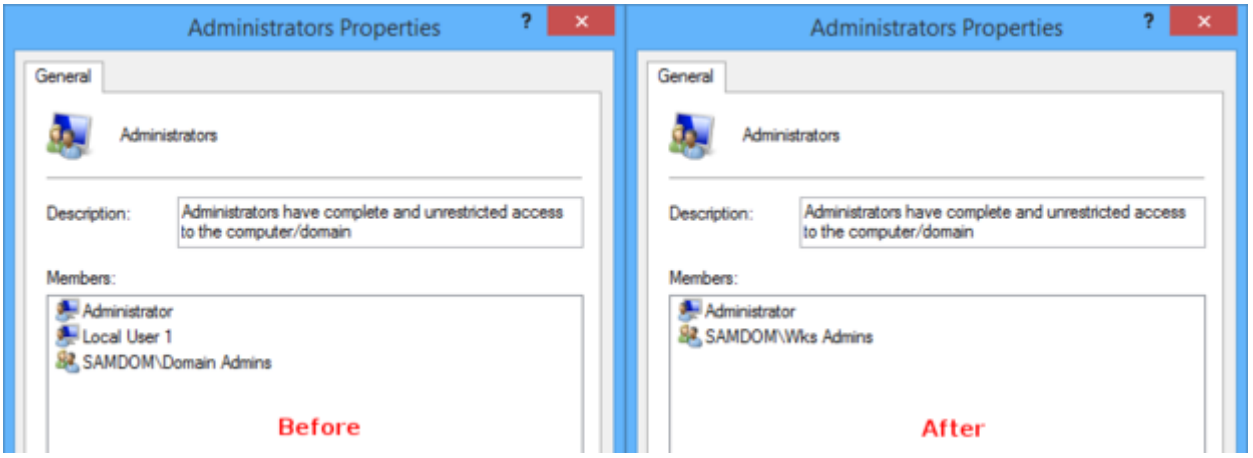


- You see the local „Administrator“ account and the AD group „SAMDOM\Wks Admins“ in the „Members of this group“ list.



- Click „OK“.

After the clients have re-read the changed group policy, only the local „Administrator“ account and then domain group „SAMDOM\Wks Admins“ will appear in the local „Administrators“ group on each client affected by the GPO. All previous members have been replaced by this new members.



Force manual group policy refresh

Windows computers refresh and apply group policies on changes per default every 90 minutes with a random offset of 0 to 30 minutes. See http://technet.microsoft.com/en-us/library/cc940895.aspx.

To see if changes took effect, you can force an immediate refresh of all GPOs on a host by running:

```
> gpupdate /force /target:computer
```

The „/target:computer“ option reads only the „Computer Configuration“ part of GPOs.

Retrieved from "https://wiki.samba.org/index.php?title=Managing_local_groups_on_domain_members_via_GPO_restricted_groups&oldid=11360"
