Windows

Domänenbenutzer zum Lokalen Administrator machen

This how to will walk you through using Restricted groups to put users in the local admin group on all PCs. It will also add them to the Remote Desktop user's group.

The usefulness in this is keeping as many people out of the domain admin group as possible while allowing the techs to work.

I see this in forums every once in a while but since I am revamping some policies with 2008R2 I thought I would take the time to write down the steps to do this handy little procedure.

I have created these instructions for 2008R2 it should work with 2003 just fine but if you need more details on 2003 check my reference below.

Steps (4 total)

1 Define Security Group

First you need to define a security group in AD users and computers. In this example I am creating a security group called IT_Admins

1. Log onto a Domain Controller

2. Right click Users, New->Group->Security Call it IT_Admins

3. Add the proper members. I will add myself, Optimus, and Zelda.

2 Create Group Policy.

Next you need to create a group policy or use the default Domain Policy (not recommended).

For this example I am creating a separate policy called "Local Administrators"

1. Open Group Policy Management Console GPMC.MSC

2. Right click your domain or OU.

3. Click Create a GPO in this domain, and link it here.

4. Call it "Local Administrators"

5. You should see the policy in the tree now.

3 Edit the policy to contain the IT_Admins group

Here you will add the IT_Admin group to the local administrators policy and put them in the groups you wish them to use.

1. Right click "Local Administrators" Policy.

2. Expand Computer configuration\Policies\Windows Settings\Security Settings\Restricted Groups

3. In the Right pane of Restricted Groups, Right click and hit "Add Group..."

4. Type IT_Admins and hit 'OK"

5. Click Add under "This group is a member of:"

6. Add the "Administrators" Group.

7. Add "Remote Desktop Users"

8 OK

*NOTE: When adding groups, you can add whatever you want, the GPO will match the group on the PC, if you type "Princess" it will match a local group called princess if it exists and put "IT_Admins" in that group.

**NOTE: If you chamge "Members of this group:" it will overwrite the accounts you set up in step 1.

4 Test

Wait 15 minutes, or log on to a PC and type gpupdate /force and check the local administrators group. You should see IT_Admins in the group now.

Optimus and Zelda can now access all PCs remotely as a local administrator.

Eindeutige ID: #1001
Verfasser: Roman Festl
Letzte Änderung: 2016-08-08 17:20