

Re: Local admin through group policy and keep admin on local machi

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-03/msg01473

- *From:* "Al Mulnick" <amulnick_No_SPAM@xxxxxxxxxxxxx>
 - *Date:* Thu, 22 Mar 2007 19:52:12 -0400
-

When you say "Beta server" What does that mean to the rest of us exactly?

"Kevin Rhodes" <KevinRhodes@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:C9F8B4E1-85BC-498A-954A-7B5D0F583199@xxxxxxxxxxxxxxxxxxxxx

Thanks for your help Roger!

I think that you understand our situation correctly. When it comes to implementaion, I am a little confused about how to add members to the Support group and limit them only to this OU.

The user group is: "Support" and it is a member of administrators (built-in)
My current GPO for the OU is: Resticted group, "Support"
The member of this GPO is the domain's group: "Support"

If I add user accounts to the domain Support group, they don't have local admin. You mentioned: "If you want to control the domain accounts that are members in Support, do this in a GPO that has the DCs OU within its scope." Can you walk me through that part?

BTW-This beta server does not have SP1 or SP2 installed at present.

Thanks again,
Kevin

"Roger Abell [MVP]" wrote:

The way I am hearing this is that you need a custom support group to always be in the machine local Administrators group on all of a set of machines that you have in an OU, and then, on some of those machines you also need to have the domain

Re: Local admin through group policy and keep admin on local machi

account of a user of the machine, and this last part differs per machine.

How I would go about this is via Restricted Group definition in GPO for the custom support group, and then adding the per machine domain account via script (just run at cmd prompt) or via manual addition if number of machines needing this is small. To add the custom support group, let us say it is named Support, a domain group, use a GPO that is linked to the OU and in it define as a Restricted Group "Support" (yes, not Administrators but Support, the group to be added to each local Administrators group). In the Restricted Group definition leave the Members list empty, and in the Member Of list add Administrators.

If you want to control the domain accounts that are members in Support, do this in a GPO that has the DCs OU within its scope. The GPO linked to the OU will make sure that Support is in Administrators and it will not cause anything that is already in the machine local Administrators group to be removed.

If you then add the per machine domain account as/where needed it will stay a member of Administrators. If that domain user removes Support from their machine's Administrators group the Support group will be restored as a member as soon as the GPO is reapplied.

As far as you wanting to immediately refresh policy, it sounds like you have tried gpupdate on the client but not find it to work. If that is the case it may be that you did this before the changed GPO had replicated to the DC preferred by that client. Make sure that you use the /force switch.

Roger

"Kevin Rhodes" <KevinRhodes@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message

news:1E4FAEDB-40EC-4196-8A25-899DA211AF5C@xxxxxxxxxxxxxxxxxxxx

I have created a local admin group policy giving a group admin rights over an OU (this is to be for our help desk). Some of our software programs require users to have local admin access as well (so I give it to them through their domain account on the local PC—I don't want to add them to help desk group and give them local admin on all the OU PCs). The problem is that the following day the admin account on the local PC is automatically

Re: Local admin through group policy and keep admin on local machi

removed
from
the list of administrators. I have this set up in a beta
environment so
we
don't have to go to each machine, each day, to add them back
in. Any
ideas
on
how to block this? I have tried to turn "no override" on in the
GP
options,
but this too disappears the following day. Is there anyway I
can speed
up
whatever cycle time it is on so that I don't have to wait a day
to see
if
it
works? (I always do a forced update after I make changes).
Thanks in
advance.