

Re: no Domain Admin rights to a Domain Server

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2006-08/msg00014.html>

- *From:* "Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 21 Jul 2006 23:56:49 -0500
-

If the computer is still a member of the domain with proper DNS name resolution and network connectivity [no interfering software firewall, etc] then you should be able to gain access again. But if he removed it from the domain then you no longer have any control over that computer. Also if he disabled the workstation service then Group Policy would not work. You could try using nltest to see if the computer still has a secure channel to the domain controller. If it does not then it probably is not a member of the domain anymore. The link below on nltest is a little old but I believe the examples are still correct or you can use nltest /? to see the syntax for nltest.

<http://support.microsoft.com/kb/158148/>

Assuming it is still a member of the domain you could try using either a Group Policy "startup" script with the net localgroup command to add domain admins to the local administrators group as in net localgroup administrators "domain\domain admins" /add . The problem with that approach is that it would not take effect until the computer is restarted. The other approach would be to create an OU with a Group Policy linked to it that had Restricted Groups configured so that domain admins is a member of administrators. Then you move that computer account into that OU and wait. If the computer is not rebooted Restricted Groups will eventually apply but could take up to two hours if the computer is using the default Group Policy refresh intervals. See the link below on a good explanation on how to implement Restricted Groups and I would put one other test computer into the OU also to see if RG is working or not. You could reboot the test computer or run gpupdate /force on it to see if RG is working instead of waiting until the refresh interval. You will need to get the powers that be involved to put an end to this cat and mouse game. If the computer is not a member of the domain it needs to be joined to the domain again and the domain admins group will be automatically added to the local administrators group. If the user refuses to cooperate see the second link below on how to reset the local administrator password so that you can gain access assuming that syskey type 2/3 has not been enabled.

Steve

<http://www.windowsecurity.com/articles/Using-Restricted-Groups.html>
http://www.petri.co.il/forgot_administrator_password.htm

Re: no Domain Admin rights to a Domain Server

"Donald Palmer" <DonaldPalmer@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:C995AC9B-72D6-45F1-8502-2ECA073C958C@xxxxxxxxxxxxxxxxxxxx

I have seen a similar scenario to this one but the suggestions did not work in my case. I am the Domain Admin of the servers and the DomainName\Administrator account has had its rights taken away on a specific server. I can logon locally to the machine but the rights are that of a regular user.

Basically, the server belongs to engineering and the person in charge there has removed access from anyone but himself. He does not have Domain Admin rights but he was able to take control and remove any rights from anyone else. Management is looking at this but I have been tasked with gaining access back.

I tried to implement Group Policy and give back rights to the local admin group with the restricted Group but this did not work as the server seems to not have any permissions to run or query Group policy.

Other than formatting the server and re-installing is there a way to gain access over the server given admin rights on the domain?

--
Donald Palmer, MCSE