

Re: Can not log on to domain controller remotely or locally.

Re: Can not log on to domain controller remotely or locally.

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2008-10/msg01306

- *From:* Paul Bergson [MVP-DS] <pbbergs@xxxxxxxxxxxxxxxx>
 - *Date:* Fri, 24 Oct 2008 17:26:35 +0000 (UTC)
-

Hello s13james,
Sounds like you may have replaced who is in the domain admins group.

From a command prompt within your domain

```
net group /domain "domain admins"
```

Hopefully you can use a name from this group to gain access to your DC

+++++
Below is some info on how to setup Restricted Groups, if you do it wrong it doesn't merge members it replaces them.

To use the restricted user group gpo setting

```
computer configuration \ windows settings \ restricted groups
```

```
group = your group to be made local admins member of = BUILTIN\Administrators
```

<http://www.windowsecurity.com/articles/Using-Restricted-Groups.html>

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/librar...>

<http://www.microsoft.com/resources/documentation/windows/xp/all/prodd...>

There is absolutely nothing that has to be done on the client side.

Re: Can not log on to domain controller remotely or locally.

Re: Can not log on to domain controller remotely or locally.

Create the gpo in the ou where the Computers reside (NOT the users), go to computer configuration/windows settings/security settings/restricted groups, right click on restricted groups and select new group (For the local computers, this group name should be – administrators) and key in the group you want auto populated. Select add on the Members of this group and then add the members you want populated.

Note: Be aware that the higher you place this setting within the domains group policy the possibility exists it is applied to machines you may not want it applied to. With this in mind you should try and avoid this setting at the domain level, with the exception on the domain admins group. We have some users who are local admins on machines and for some reason they feel compelled to remove the domain admins from their local administrators group. Setting this at the domain level manages these annoying users.

--

Paul Bergson
MVP – Directory Services
MCTS, MCT, MCSE, MCSA, Security+, BS CSci
2008, 2003, 2000 (Early Achiever), NT4

<http://www.pbbergs.com>

Please no e-mails, any questions should be posted in the NewsGroup This posting is provided "AS IS" with no warranties, and confers no rights.

So I have been working out some issues with our domain controller that were preventing us from joining the domain. I got that working last week sometime and all has been well for the past week, so I decided to start working on editing our security policies in order to get ready to join the rest of our users to the domain (currently I'm the only domain user). With that in mind, yesterday I edited the password policy since the default Server 2003 password policy is pretty harsh. I also experimented with a way to make all users local administrators of their machines via Restricted Groups. I believe this may have been where my issue comes in.

I leave for the day yesterday, all is well, I come in this morning and try to remote desktop into the server and I get the message "To log on to this computer, you must be granted the Allow log on through Terminal Services right." This seems odd, since I've never modified this setting and I've always been able to connect through Remote Desktop. So I think no problem, I'll just walk over to the server and fix it at the machine itself.

I sit down at the machine and notice that it has restarted overnight, it's scheduled so no problem there. I attempt to log in and I get the message "The local policy of this system does not permit you to logon interactively." Oh crap.

Re: Can not log on to domain controller remotely or locally.

Re: Can not log on to domain controller remotely or locally.

So at this point, I can't log into the server at all. I try every account I know of and not a single user account works to log on. It seems almost like all of the accounts have lost domain admin privileges because I get Access Denied every time I try to manage the server remotely using MMC snap ins.

Anyone have any recommendations or am I dead in the water? Please be the former... we have the SVN repositories for our game studio on that server.

Oh, and by the way, all services seem to be working fine. Our SVN hosting, wiki, and bug tracking systems are working fine. I just can't get into the server to do any management.