

microsoft.public.win2000.group_policy: Re: Local policy does not allow interactive login

Re: Local policy does not allow interactive login

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.group_policy/2004-09/0216.html

From: Steven L Umbach (*n9rou_at_n0-spam-for-me-comcast.net*)

Date: 09/09/04

Date: Thu, 09 Sep 2004 16:20:08 GMT

Hmm. I am not sure what the exact problem is but if the server you took offline was a domain controller that certainly can cause problems with domain policy replicating and being applied properly.

If this is a native mode domain, the users will need to be able to access a global catalog server in order to logon so you may want to verify that one is available if you are in native mode as shown in Active Directory Users and Computers. Right click the domain and look in properties to see what mode it is in.

<http://support.microsoft.com/default.aspx?scid=kb:en-us:816105> --- same for W2K

Dns configuration is critical in an Active Directory Domain. Shutting down the old dc could have upset this. In short domain controllers must point to themselves or pdc fsmo domain controller as their preferred dns server in tcp/ip properties as shown by Ipconfig /all. Domain members must point to only domain controllers running dns with the AD domain zone which all do in W2K by default. Possibly they were pointing to the old dc?? Use Ipconfig /all to find out and you may need to adjust DHCP scope to reflect any changes. See the link below on FAQ for AD dns.

<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B291382>

<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q294328> --- may be of help.

The fact that you can not access Domain Security Policy may be due to the fact that the pdc fsmo can not be reached and may have been your old dc? See the link below for more info on that error.

<http://support.microsoft.com/?id=294257>

<http://support.microsoft.com/default.aspx?scid=kb:en-us:197132> --- explanation of the five fsmo role holder.

I would use the support tools netdiag and dcdiag to check the general health of your domain configuration. First run netdiag and then dcdiag on a domain controller looking for any pertinent errors. Also look in the Event Viewer of your domain controllers for any errors that may indicate a problem with replication, etc. Use netdiag on a domain member computer looking for any errors that may indicate a problem particularly for dns, dclist, kerberos, and secure channel. Hopefully some of this will provide a clue for you. --- Steve

Re: Local policy does not allow interactive login

<http://support.microsoft.com/default.aspx?scid=kb:en-us:321708> — netdiag and how to install support tools.

"Dave" <dave_advantage@hotmail.com> wrote in message
news:%234ypFenIEHA.3876@TK2MSFTNGP15.phx.gbl...

>> *There have been various worms that use secedit to reset the user rights on a
>> computer so you may want to make sure the computers are clean and use Autoruns
>> from SysInternals to see if there any strange startup entries for these computers.*

>>

>> <http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml>

>

> *There doesn't appear to be anything out of the ordinary running on startup. I've
> also performed a virus sweep on the network and that came up with nothing also.*

>

> > *The other thing to try is to define the deny logon locally user right.*

> *You can define*

>> *it and leave no entries or I usually add the guest account to the list. In*

>> *addition enable auditing of policy change on those computers and then check the*

>> *security log in Event Viewer for "policy change" events under category such as*

>> *Event ID 622 that may help you track down what is going on. It is curious that it*

>> *is not affecting the Windows XP computers. --- Steve*

>

> *I've defined the Deny Logon Locally policy on both the Domain Security Policy and*

> *the Domain Controller Security Policy and put only Guests in the list. I don't see*

> *anything out of the ordinary in the Event Viewer.*

>

> *Here's one other curious piece to the puzzle...The old antivirus server is listed*

> *as a Domain Controller when I look in active directory. I don't think it was a DC*

> *before and I'm sure that I've never promoted it. I've not been doing this job for*

> *very long, so it's possible that it may have been there before, but I wouldn't*

> *think you would want an antivirus server as a DC. Anyway, when I try to go into*

> *either Domain Security Policy or Domain Controller Security Policy, I get an error*

> *saying "Failed to open the Group Policy Object. You may not have appropriate*

> *rights. Logon failure: the target account name is incorrect". Now when I take*

> *this machine offline, my users still get the "interactive logon" error message. So*

> *it doesn't matter if that server is up and running or not. However, when it is up*

> *and running, they are also not able to connect to the PDC, though they can*

> *eventually get logged into the domain. Could it be that the other machines are*

> *trying to pull down the security policy from this server and are unable to, thus*

> *causing the "interactive logon" error?*

>