

Re: Domain Users into Local Admins

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-04/0365.html>

From: Todd J Heron (todd_heron_no_spam_at_hotmail.com)

Date: 04/22/05

Date: Fri, 22 Apr 2005 07:17:50 -0400

Sometimes two reboots are needed. Failing that, see below.

The following are common reasons why GPO settings are failing to apply to a user or computer (8-point check):

- 1) Machine or user must be a domain member and authenticate with the domain
- 2) DNS client configuration problem. Is the client's preferred DNS server setting pointing to a DNS server that handles the zone for AD domain
- 3) User or machine is not in the container to which the GPO is linked. Run `rsop.msc` or `gpresult.exe /v` on the users workstation to check that the policy is actually being applied or not.
- 4) User or machine is under a hierarchy which is blocking the GPO
- 5) There is group filtering which is preventing the user or machine from reading the GPO
- 6) The user is a member of a group which is being filtered from the effect of Group Policy. For example, the 'Authenticated Users' has "Deny" selected for 'Apply Group Policy'.
- 7) If ICMP is blocked for administrative reasons, group policies will not apply. (Clients test the link speed by sending an ICMP packet of 2048 bytes.)
- 8) Check to see if the user is a member of too many groups.

Quoted from:

Kerberos authentication may not work if user is a member of many groups:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;280830>

If a user is a member of many groups either directly or because of group nesting, Kerberos authentication may not work. The Group Policy object (GPO) may not be applied to the user and the user may not be validated to use network resources.

--

Todd J Heron, MCSE
Windows Server 2003/2000/NT; CCA

This posting is provided "as is" with no warranties and confers no rights