

Re: Domain Administrator privs on Client

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2006-02/msg00174.html

- *From:* "Tim Guy" <tim@xxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 15 Feb 2006 11:28:17 -0000
-

OK. I understand Restricted Groups.

But I dont understand how that will help me allow domain admins and domain administrators to be able to act as administrators of loca machines. Unless you're telling me that the domain admins and administrators are already in a group somewhere that I dont know about?

IE. I have an SQL server on my domain, I have to login as the local sql administrator to do most admin task. Id rather use the domain administrator account to do these things but it wont allow me to do it saying that various things along the lines of "You do not have the prilvages to install this", etc, etc....

Tim

"Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> wrote in message <news:e039MpdMGHA.1488@xxxxxxxxxxxxxxxxxxxxxxxx>

The Enable to delegation setting is quite something else.
If you have enabled that due to this reasoning you should reverse it.
That setting lets the accounts assume the credentials of others in circumstances where they have the token available.
This is a potential risk if given to any principal that is not regulated.

Restricted groups is the group policy way to dictate the complete list of members in (of the memberships of) a group.
However, be aware that this is the full list and will replace any other memberships.

One can set a machine startup script to check that Domain Admins is still a member of its machine local Administrators group and if not then add it. This leaves a window of time, between restarts, when the Administrators might be altered, whereas Restricted Groups for a member will in default circumstances have a window of about 90 minutes max.

"Tim Guy" <tim@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:ePpMwhXMGHA.2580@xxxxxxxxxxxxxxxxxxxxxxxx>

Re: Domain Administrator privs on Client

With Windows 2003 AD/Network, I can not get a domain administrator to administer a local client / server. Only the local administrator will work.

I always thought that the setting in windows 2000 GPOs to over come that was "Enable Computer and User accounts to be trusted for deligation"

Doesnt seam to be on Windows 2003. What is the policy setting in a GPO to get around this?

Cheers

Tim