

Re: FOR A SKILLED IT EXPERT – WIN2K SERVER – DOMAIN CONTROLLER

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2006-03/msg00052.html>

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Wed, 8 Mar 2006 15:37:57 -0700
-

So then the policy is disallowing all login by all users at all machines ?
The remote tools would need to be run with a recognized domain account having admin priv in order to edit the group policy objects. That pretty much makes running from a CD boot not an option. I had thought that with Windows 2000 one could not block the built-in Administrator account from being able to log in (while in Windows Server 2003 one can, but not from a safe mode boot). The built-in Administrator account may have been renamed, but if you know what the account is then perhaps this will give you a route to log in.

"West-Wind-7" <WestWind7@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:A5E710B2-AC12-4172-B770-9BBD2906545F@xxxxxxxxxxxxxxxxxxxx

Thank you and Bless you Roger for your time in answering – VERY much appreciated.

Will soon attempt your suggestion if we can access the Server from the workstation.
(last message denied access to the server from the workstation – the WKSTN boots up on cached profile only) The interactive logon problem has applied to ALL users in the Domain.

Yes – it is very possible we are at a pre-DC state on the server after the manual security reset.

Yes – we have a very recent back up of the system state, but how do we logon to use the tape deck (Dell SCSI) ??

Worst case Roger, can we use the tools suggested from a CD Rom or floppy boot?

God Bless you again and thank you again....

Take care –

WW7

"Roger Abell [MVP]" wrote:

The message is referring to the effective policy.
The setting could originate anywhere.
NTrights pokes the effective setting and gives you on a DC
a 5 minute window to log in. You need to find which GPO
this was set in and change it back.
If you need, you can define a temp GPO linked onto the DC OU
at highest priority that sets a value of Administrators as having the
log on local user right in order to not hassle with things while finding
and changing back what had been set accidentally.

However, you now have other issues due to the effort with resetting
the security. I am not quite sure where things are at for you now
since that probable tweaked things back to pre-domain controller
config. Can you install the adminpak.msi (www.microsoft.com/downloads)
on a machine in the domain and use the mmc tools to get at the config
of the domain remotely ?? Also grab GPMC while you are at downloads.

If you had not tried the reset we could have pulled you out of this, per
the
comments of the opening paragraphs and remote tools. With the reset
attempted I do not know. How far did things get and what happened??
The best chance at this point may be if you have a recent valid full
backup
of the system state so that an authoritative restore could be done.

Hopefully others reading this have some ideas . . .

It is sometimes useful to disallow admins local login.
That can be a valid and desirable deployment.
MS cannot anticipate what is unlikely a useful configuration and
make the settings for same impossible, although in a very few
cases they have, since as soon as it is said "that is not a valid
thing to do" a situation comes along in which it is.
That said, it is possible, and I have seen, Domain Admins completely
locked out from all ability to log into or manage their forest. Sort of
foolish, to do and to allow to be done, but I guess it is a case of at
what point do you allow and disallow.

"West-Wind-7" <WestWind7@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in
message
news:88C35619-1C73-4095-8E11-949155242A39@xxxxxxxxxxxxxxxxxxxx

Thanks Roger – The error message says the LOCAL
POLICY..But it is true
that

Re: FOR A SKILLED IT EXPERT – WIN2K SERVER – DOMAIN CONTROLLER

the Domain Policy was edited but NOT the logon rights for any user.

Used NTRIGHTS over the network, and that fixed it once. BUT, each time i (Administrator) logged on the same problem came back.

So, i followed the MS instructions to manually edit the inf and ini security files to reset everything back to default.

Still the same error message. NOW, NTRIGHTS will not work – so network access is not an option.

We are a small 2 pc design Company also engaged in Christian Evangelism.

It looks like i must install another copy of the OS in a separate folder and boot up through that, and then manually edit the files.

Unless you can think of another way??

REGARDING your comment : > If there were a simple way to reset everything when the system

believes you are not entitled to do so it would not be a very well planned system design now would it ?

WHY WOULD THE SYSTEM DENY THE ADMINISTRATOR LOGON RIGHTS???

If the Admin can't get in the system is useless.

Why would the system NOT warn an Admin that the changes made to the policies will PREVENT him from logging back on??

It is a conundrum, and having scoured the internet, multitudes of other

people have experienced this very same issue.

CONCLUSION : It is an MS flaw in the way the OS responds to Security Policy changes made by an Administrator who is NOT a Degree Holder in Computer Science. The OS MUST tell the person, BEFORE the changes are absorbed, that doing so will LOCK THEM OUT OF THE SYSTEM...

It does not do that, otherwise i would NOT be in this mess.

If you have any other ideas of how to reset the security back to default, with ZERO Domain access we would ALL love to know,

Bless you Roger and thank you for your reply ... very much appreciated...

In Christ and in Truth...

WW7

"Roger Abell [MVP]" wrote:

You have told us this is with Windows 2000 server.

However, your subject says Domain Controller, but your message says the change was in the local security policy, which is not used on domain controllers.

What is it that you modified ?? If it was only the Log on Locally and/or the Deny log on locally policies, then just edit the GPO remotely over network with a domain admin account and reverse the changes.

If there were a simple way to reset everything when the system believes you are not entitled to do so it would not be a very

well planned system design now would it ?

"West-Wind-7"

<WestWind7@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message

news:8A59B55E-6062-429D-B146-F958EC25532B@xxxxxxxxxxxxxxxxxxxx

"The local policy of this system does not permit you to logon interactively"

Hello Everyone – i made a small and insignificant change to the local security policy. NO ERROR MESSAGE, that i would be locked out of the server, and for this i am very upset with MS.

Anyhow, i CANNOT logon with ANY USER, not even the built in Administrator in Directory Services Mode. This has been for over 10 days now. DO NOT WANT TO LOSE the profiles.

Does ANYONE know of a floppy boot up program that will RE-SET all Domain Controller Security back to DEFAULT???

Re-setting the Password is not the issue.

How CAN all SECURITY be reset to default, via a boot-up floppy program to

Re: FOR A SKILLED IT EXPERT – WIN2K SERVER – DOMAIN CONTROLLER

allow logon normally again
without this RIDICULOUS
MESSAGE "The
local
policy
of this system does not
permit you to logon
interactively"

SURELY, there is a way to
easily reset the security?

Hope someone can suggest
something...

Thank you and God Bless
you...

West-Wind-7