

Locking down TS on Domain Controller...

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.terminal_services/2006-07/msg00169.html

- *From:* "Cary Shultz" <cwshultz@xxxxxxxx>
 - *Date:* Sun, 9 Jul 2006 10:58:58 -0400
-

Good morning!

Okay. I know that this is not suggested. I know that it is not recommended. I am aware of the security risks. I know that there are several people who will kill me when they read this. The environments that I manage are all very small and have a limited budget for 'computer stuff'.

I have a client (very small) that has a 64-bit Domain Controller (Windows Server 2003 x64 running on a Dell PowerEdge 800). They have a remote office and they want to use Terminal Services so that those five users in the remote office can access vital information. Pretty much nothing else is of interest to them.

So, I would like to lock down the Terminal Server experience for those five users. Just as a point of interest, I have done this several times in a WIN2000 environment and once in a WIN2003 environment (following the usual MS KB Articles and Patrick Rouse's suggestions on the File System – all works very very well). The *MAJOR* difference was that in each case the TS was a member server, not a Domain Controller.

I should mention that I am playing in the lab right now. The only difference between the lab and the production environment is that I am sitting on a 32-bit Server right now. I will not be able to use the GPMC when it comes time to do this on the production server as the GPMC does not run on 64-bit Servers....

Everything (minus the TS Lockdown GPO) is working. So, there are no other issues (well, none that I can see). I have a WINXP Pro SP2 client and I log on to that using the user account object of one of the five TS Users and then use RDP to connect to the Terminal Server. Everything is good (again, minus the lockdown GPO).

Here is what I have done:

Follow MS KB278295 (create the GPO, link it to the Domain Controllers OU – I know, I know, use gpupdate /force and then log on as one of the users. None of the settings set by the 'TS Lockdown' GPO take place). I have done this, as I already mentioned, in production environments several times as well as

Locking down TS on Domain Controller...

in the lab hundreds of times. When I run RSOP.MSC on the Domain Controller and change the focus (from Administrator to TSUser1) I do not see any of the settings set in the 'TS Lockdown'.

Oh, one more point – on the SECURITY tab of the GPO I removed Authenticated Users and 1) replaced it with a security group that I created (which contains the user account objects) – nothing, 2) replaced that security group with 'Remote Desktop Users' (just to see if that had any effect) – nothing, and 3) removed the group and replaced it with each individual user account object – nothing! After each of the mentioned changes I used gpupdate /force and, when nothing happened, I rebooted the Domain Controller (again, in the lab right now). Still nothing.

There is nothing in the event logs to indicate the GPO failed for such and such a reason. This is a bit odd!

I guess that because this is a Domain Controller I am getting stupid!

Does anyone have any suggestions?

Thanks all,

—

Cary W. Shultz
Roanoke, VA 24012