

Re: Error 15401 using sp_grantlogin (not addressed by current KB articles)

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2002-10/2686.html>

From: Trevor Scroggins (trevor.scroggins@homeqabc.com)

Date: 10/02/02

From: "Trevor Scroggins" <trevor.scroggins@homeqabc.com>

Date: Tue, 1 Oct 2002 17:28:22 -0700

Hello, Bill. Thanks for the response! One problem though—there isn't a reference to DOMAIN\oldusername in sysxlogins. That's why I'm confused. Restarting Windows 2000 resolved the problem for this particular account, but if I add a new account and rename it (or rename the first account a second time), the problem returns. I'm not sure where our authentication failure came into play as I took over the problem after the DBAs had tried sp_revokelogin and sp_grantlogin. I'm still wondering why get_sid returns NULL for an account that exists. I'm assuming it's using some sort of internal cache that's storing the old name and SID combination and getting confused when it sees a duplicate SID.

It turns out our company has a premier support agreement, so I've gone ahead and opened a support instance. I have a feeling they'll decide that rebooting the server fixed the problem, but that won't satisfy me. :-)

I'll forward your response onto our database group for discussion. Thanks again!

Trev

""Bill Hollinshead [MS]"" <billhol@online.microsoft.com> wrote in message news:Q3f3kWZaCHA.364@cpmsftngxa06...

> *Hi Trevor,*

>

> *Get_sid() does exactly that <g>, when an account name is supplied as an argument to get_sid, it returns a sid. Sysxlogins contains two relevant columns: sid and name. The sysxlogins.name column stores the NT account name that was in existence *when the account was added to SQL Server* (i.e., DOMAIN\oldusername). When an NT Domain Admin renames an account (using NT tools, and as opposed to dropping and recreating an NT account also using NT tools), NT will retain the original sid and simply rename the account. Thus the problem: NT has the original sid with DOMAIN\newusername while SQL Server's sysxlogins..name still has the original sid with DOMAIN\oldusername.*

- >
- > *One way (the safest method) to get SQL Server to agree with the renamed NT*
- > *accounts is to script out the logins (once for the system), users (once*
- for
- > *every database), and the users' permissions (once for every database).*
- This
- > *is done via SQL Enterprise Manager's menu after selecting a database,*
- > *choose Tools/Generate SQL Scripts, on the General tab click Show All and*
- > *check "Script all objects", on the Formatting tab UNcheck "Generate the*
- > *DROP <object> command for each object", on the Options tab check*
- everything
- > *(4 boxes) under "Security Scripting Options", back to the General tab*
- click
- > *Preview (to ensure the script was created), and then save the script. You*
- > *can then open the script within an ASCII text editor, *verify the commands*
- > *are just those commands that are desired* (the CREATE TABLE commands can*
- be
- > *deleted, but CREATE TABLE will fail if the table already exists), and*
- > *replace DOMAIN\oldusername with DOMAIN\newusername (apart from where the*
- > *script drops DOMAIN\oldusername). Then backup all databases and run the*
- > *script. *If the script edited and verified properly*, it should drop*
- > *DOMAIN\oldusername, create DOMAIN\newusername, and assign appropriate*
- > *permissions to the appropriate objects. This script is worth archiving (as*
- > *would be a complete script of all user databases) in a safe location. Make*
- > *sure to test upon a sacrificial SQL Server system before trying this in*
- > *production. Some of that editing can be avoided, and some of this*
- > *management overhead/pain can be minimized, by having originally used NT*
- > *Groups instead of using individual NT logins – perhaps too late at this*
- > *time, though <g>.*
- >
- > *Alternatively, you should be able to ignore this issue since the NT*
- > *accounts should be able to connect to SQL Server via their*
- > *DOMAIN\newusername even though DOMAIN\oldusername still exists in*
- > *sysxlogins (i.e., you don't really need to sp_revoke and sp_grant logins*
- > *since it is the sid that matters and it is the sid that gets passed to SQL*
- > *Server from a client). This is why the issue is not observed by many DBAs*
- > *(unless the Authentication problems started happening at about the same*
- > *time that the NT account names were renamed). If you are seeing*
- > *authentication issues, perhaps the issue is really/instead that the client*
- > *cannot currently see the domain controller, and thus the login account's*
- > *sid cannot be passed to SQL Server from the client – this normally would*
- be
- > *evidenced by a logon failed for user NT authority\anonymous (on a SQL 2000*
- > *domain) or by logon failed for user NULL (on an NT 4.0 domain) being*
- > *returned by SQL Server within it's logon failed error message. If logon*
- > *failed for user NULL is being seen, then it is likely better to ensure*
- that
- > *client box can see the Domain Controller, and be authenticated by that DC*
- > *(i.e., an NT issue). For example, a SET command will return the*
- LOGONSERVER
- > *environment variable which is populated at the last system startup, and if*

- > LOGONSERVER is equal to the client box's name then (when NT was started)
- > the DC could not be found and cached credentials were instead used. Thus
- it
- > is likely better to ensure the account upon that client box has logged
- onto
- > a freshly recycled NT with the DOMAIN\newusername. If that logon after a
- > recycle fails, then the this issue is clearly an NT/Domain Authentication
- > issue (at the client) since the account cannot logon to NT, and is not a
- > SQL Server using NT Authentication issue (which should be expected to fail
- > if a client cannot authenticate with a DC).
- >
- > Finally, you may be able to find newsgroup scripts that update sysxlogins,
- > but please be aware that such ad-hoc updates to the system catalog can
- > cause, and have caused, unexpected system behavior and thus are not
- > supported. If you want to risk trying such a script, then I strongly
- > suggest backing up the master database before running it, and I suggest
- > testing the system after running it but before the backup becomes obsolete
- > (obsolete perhaps because new logins were added to master since the backup
- > was made, etc.). Personally, I would rather play it safe and follow the
- > supported yet slower route within the 2nd paragraph of this response.
- > Finally, if such a script were run and if the NT Authentication problems
- > still exist, then the cause could either be that update sysxlogins, or the
- > cause could be the original (still unresolved) NT Authentication issue –
- > this is sort of a "one step forward two steps back" situation, for which
- > rebuilding the master database may be the more sure-fired (and
- unpalatable)
- > means to resolve which issue is the cause (and perhaps still needing to
- > resolve the client NT Authentication issue).
- >
- > If you need further help, please feel free to contact me offline (remove
- > 'online.' from my alias). In a production server situation, it is perhaps
- > far better that you open a case with support as their help will be more
- > immediate. Be sure to mention the impact upon production.
- >
- >
- > Thanks,
- >
- > Bill Hollinshead
- > Microsoft, SQL Server
- >
- > This posting is provided "AS IS" with no warranties, and confers no
- > rights. Subscribe to MSDN & use <http://msdn.microsoft.com/newsgroups>.
- >