

Re: Complete Neophyte Question(s)

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2007-07/msg00023.html>

- *From:* "James" <minorkeys@xxxxxxxxxx>
 - *Date:* Mon, 9 Jul 2007 10:16:44 -0400
-

That makes complete sense to me, but somehow I'm overlooking something.

I have a user named james on a database. If I go into properties for that user they have no owned schemas. They have no role membership (including public, which isn't listed here for some reason). If I right-click the database and go to properties -> Permissions, the only permission they have is Connect, not view definition.

The only thing I can see is that there's a login of the same name at the server level which is a member of the Server Role public, but my understanding is that it's unrelated.

So the long and the short of it, is that this user can view definition on this database, and I can't figure out why.

"Erland Sommarskog" <esquel@xxxxxxxxxxxxxx> wrote in message [news:Xns996668C8847CBYazorman@xxxxxxxxxxxxxx](mailto:Xns996668C8847CBYazorman@xxxxxxxxxxxxxx)

James (minorkeys@xxxxxxxxxx) writes:

Disregard, seems my google-ing skills were lacking.

You should not have to go Google to find out what WITH GRANT means. SQL Server comes with online documentation on you hard disk.

WITH GRANT is one of the more esoteric features in SQL Server in my opinion, but maybe that says more about the simplistic security of the system I work with.

More generic question as I'm messing with the Northwind database to get a thorough understanding of this. If a user isn't a member of any roles and has no permissions explicitly defined, does it err on the side of deny or grant? Or does that depend on the permission? Right now I have a user who has Connect as the only database level permission, no roles, no secureables but can still view definition, it seems. I'm able to connect and view all of the tables, although everything else seems locked down. I have refreshed and can still see them.

Re: Complete Neophyte Question(s)

If no permissions have been granted, then you have no permissions. That is, if run the below in a database, the SELECT should not return anything:

```
CREATE LOGIN erik WITH PASSWORD='äertsoppa'  
go  
CREATE USER erik  
go  
EXECUTE AS LOGIN = 'erik'  
go  
SELECT name FROM sys.objects  
go  
REVERT  
go  
DROP USER erik  
go  
DROP LOGIN erik
```

...unless rights have been granted to the public role.

In SQL 2005 a user only has permission to see the definition of objects to which he been granted some access. More exactly he needs VIEW DEFINITION, but this permission is implied if he already has SELECT permission.

Where DENY comes in is that it overrides GRANT. Say that a user is a member of a role that has SELECT permission to a table X, but that himself he has been denied access to the table. Then he cannot access that table.

--

Erland Sommarskog, SQL Server MVP, esquel@xxxxxxxxxxxxx

Books Online for SQL Server 2005 at

<http://www.microsoft.com/technet/prodtechnol/sql/2005/downloads/books.mspx>

Books Online for SQL Server 2000 at

<http://www.microsoft.com/sql/prodinfo/previousversions/books.mspx>