

microsoft.public.sqlserver.security: Re: sp_addrolemember with Windows SQL Server Login

Re: sp_addrolemember with Windows SQL Server Login

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2003-08/0463.html>

From: Dan Guzman (danguzman_at_nospam-earthlink.net)

Date: 08/21/03

Date: Thu, 21 Aug 2003 15:22:16 -0500

> (I tried it in 2000 and it behaved as I expected,
> error)

I ran the following script on SQL 7 SP4 and SQL 2000 SP3 and received no error as long as a valid domain account was specified. I would expect you will get the same results as long as a valid Windows account is specified.

```
CREATE DATABASE DB1
GO
USE DB1
GO
EXEC sp_addrole 'UserRole'
GO
EXEC sp_addrolemember 'UserRole', 'MyDomain\MyUser'
GO
```

SQL Server apparently allows you to add a Windows account to a database role even if the account does not (yet) have access to the database. Of course, this doesn't really serve any purpose other than allowing you to run scripts out-of-order. Your resourceful developer can run `sp_grantdbaccess` (and perhaps `sp_grantlogin`) so that the user can select from the view.

IMHO, `sp_addrolemember` should at least display a warning message when the account is not (yet) a valid database user.

--
Hope this helps.
Dan Guzman
SQL Server MVP

SQL FAQ links (courtesy Neil Pike):
<http://www.ntfaq.com/Articles/Index.cfm?DepartmentID=800>
<http://www.sqlserverfaq.com>
<http://www.mssqlserver.com/faq>

"Norman" <nite_eagle@hotmail.com> wrote in message

Re: sp_addrolemember with Windows SQL Server Login

microsoft.public.sqlserver.security: Re: sp_addrolemember with Windows SQL Server Login

news:5d3593c8.0308211129.19849b9f@posting.google.com...

> At little background first...
>
> SQL 7.0 SP3
>
> I was assisting a developers with security on a view. He had to add
> several database users to the view, so I mentioned roles to him and
> provided a few of the commands. I assumed that the logins were already
> defined as users in the database, so I neglected to tell him to do
> that. After he applied the commands the Windows user could not access
> the view. He recieved the error message that he was not a user in the
> database. He is what the developer did:
>
> A login already existed Domain1\User1.
>
> Assuming Domain1\User1 was already a user in DB1 as User1, he followed
> my instructions
>
> In DB1
> sp_addrole 'UserRole'
> OK
> sp_addrolemember 'UserRole' , 'User1'
> This return the error, as it should since User1 was not a user in DB1
> User or role 'User1' does not exist in this database.
>
> Being the resourceful developer, he noticed that User1 was a NT Login
> so he tried
> sp_addrolemember 'UserRole' , 'Domain1\User1'
> Which worked??? (I tried it in 2000 and it behaved as I expected,
> error)
>
> So the SQL Server login was a member of a database role. Why did this
> work? The view that role UserRole had access to could not be selected.
> It returned the Domain1\User1 is not a valid user in DB1 message.
>
> If you look in the Users of DB1 via Enterprise Manager Domain1\User1
> is in the list. The only odd thing is that the Database Access column
> said "Via group membership" instead of permit as it normally should.
> That reads like a 6.5 message.
>
> Is this a backward compatability feature for 6.5? I can not remember
> doing this or why I would by pass the database user and map a login
> directly to a database role. Any comments?
>
> Thanks,
> Norman