

Re: Need help on how to organize users and objects

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2007-02/msg00063.html>

- *From:* Henrik Nordgren <HenrikNordgren@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 12 Feb 2007 03:49:01 -0800
-

Hi!

Yeah I have only worked as SS 2005 dba for 2 months so Im pretty new. I have worked a lot with oracle before as a developer, and there the dba assigned a personal schema to each user.

Im not too keen on the concept of roles though...

1) I definitely dont want every developer to become a sysadmin, possible a dbcreator. I could assign a custom database role to them though.

2) I dont think its a good idea to assign the db_datareader to the viewers, then they can access ANY table. The best thing is for them to tell me what tables they need and I grant them select permissions to them. Or if the users are not too technical, I create views for them.

3) One thing that still confuses me with schemas is... in sql server 2000, if a user had permissions to create stored procedures, he became the owner by default. In 2005, if a user creates an sp, which schema does it belong to? For me the most logical thing is if a user has a default schema.

For example, user A has created 30 procedures he want to share with user B. Which is the easiest way to do that in 2005?

Lots of questions....

Henrik – which is grateful for your patience.

..NET Developer

"Uri Dimant" wrote:

Henrik
Security is a huge subject in SQL Server 2005 , so I'd suggest you to spend a few days to learn it

Re: Need help on how to organize users and objects

- 1) Create two Windows Group (Dev and Viewers)
 - 2) I don't know your company's policies but you can add Dev Group to sysadmin server role to make sure that they can do any thing on the server.
 - 3) For Viewers Windows group you need to grant them access to the databases that they need and add them to db_datareader database role to view the data.
- Well if they have to run SP to get results you need to grant EXECUTE permissions for this group too

And as you said that some people from Viewers need to access 1–3 tables in database A and 6–9 tables in Database B you can assign explicitly GRANT SELECT :: permissions to the role.

I have my doubt that creating 150 Schemas is a good idea , my belief that you can operate with ROLES very well.

"Henrik Nordgren" <HenrikNordgren@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:89344D98-041F-4E77-8DD6-BB488352CD4A@xxxxxxxxxxxxxxxxxxxx

Hi!

Im not a very experienced SQL Server 2005 DBA, and not I got a really big job on my hand. Im pretty sure how to proceed with most of the stuff, but there are a few things that I need some insight on.

We are setting up a SS 2005 server that initially will hold 3 large databases which I have successfully migrated from SS 2000.

The first issue is the security. In the initial phase I have 150 users in an excel sheet that will need access to the server, all with different initial databases. The users are currently located in our active directory, hence I will be using windows authentication.

In order to create SS 2005 users I created a temptable where I imported the users from the excel sheet. Then I created an SP which basically performed CREATE LOGIN 'mydomain\myuser' FROM WINDOWS WITH DEFAULT_DATABASE=Oneofthedatabases.

Now I have all the users in my SS 2005 installation. Next is the job of assigning roles and permissions. Basically there are two roles except myself the sysadmin; developers and viewers. Developers are people that need to

Re: Need help on how to organize users and objects

create and execute procedures and such, whereas viewers are people from the company that ONLY do selects on certain tables.

Now things start to get a little bit interesting. I dont think I can use any of the predefined roles here. For example, a CEO only need tables 1–4 in database A, and another executive need tables 6–9 in database A and tables 1–3 in database B.

And the developers usually want to be able to see all tables, plus the ability to create SPs and stuff. But this depends on what project the developers are currently working on.

Now Im thinking about creating schemas, one schema for each user. And then I add whatever tables and procedures they need to their schema. This way I separate the user from the objects and get a more tier like approach? What do you think? Is this a good idea?

Im worried about creating complex trees of permissions that will be a nightmare to administrate where orphaned objects will haunt me in my dreams...

your thoughts so far?

/Henrik