

Re: Need help on how to organize users and objects

Re: Need help on how to organize users and objects

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2007-02/msg00065.html>

- *From:* Henrik Nordgren <HenrikNordgren@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 12 Feb 2007 05:34:01 -0800
-

Hi and thanks for the reply.

Yes Oracle is a bit different than Sql Server, but I think you will get the concepts easily, you seem very experienced in the world of dba...

I meant as you correctly stated that all users have access to all tables, but it is the grants that allow them to do something useful like view and alter.

As I understand sql server 2005, when you create an SP for example, then do you automatically become the owner of that SP? Your sql server user becomes the owner. It doesnt become part of any schema until you assign it. I think it differs a bit here between oracle and sql server and thats why I have some problems to really grasp it...

Yeah I know about the EXECUTE AS... but this is one other thing that i dont accept so easily, because Im used to the way we worked in oracle...

Here everything worked like: If you as a developer needed a table, sp, type or any other stuff, you sent an email to the dba and he/she grant your schema this particular object. For example, a new developer started to work. She need the COMMON database which stores tables with generic data and generic SP. All this is contained in an oracle schema with COMMON as the owner. All the dba has to do is to grant the new developer this schema and she has access.

We try to do a similar setup in sql server 2005 with generic containers. And I think the concepts are pretty much the same. Sadly we have no 2005 guru here, we all have experience only in SS 2000 and oracle.

We try to keep the borders around each user pretty tight, therefor statements like EXECUTE AS is pretty hard to swallow :-)

kind regards
Henrik

Re: Need help on how to organize users and objects

Re: Need help on how to organize users and objects

..NET Developer

"Uri Dimant" wrote:

Henrik
I have just started to learn Oracle :-))))))

>Developers are people that need to

create and execute procedures and such

Well you can assign them to DBO schema (default) , so they can create and execute .

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.

You can read ANY table but not access. Yes , you can create views and grant SELECT permissions on VIEW

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?

You did not mention that between developes we need to keep permissons too. so I think that the best way will be to create Schema to Role and then you can share obkects between users. Don't forget that there is new commnad EXECUTE AS intoduced in SQL Server 2005
<http://www.sommarskog.se/grantperm.html>

I keep thinking about the subject. Perhaps on windows level you need to create more than two group to separate users as they need access to the database
and then create an appropriate permissons for those roles in database

Re: Need help on how to organize users and objects

"Henrik Nordgren" <HenrikNordgren@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:E06B07A3-7A49-4668-9897-CE0E5A7A8601@xxxxxxxxxxxxxxxxxxxx

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 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

1) Create two Windows Group (Dev and Viewers)

Re: Need help on how to organize users and objects

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 anything 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!

I'm not a very experienced SQL Server 2005

DBA, and not I got a really

big

job on my hand. I'm 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.

Re: Need help on how to organize users and objects

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 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

Re: Need help on how to organize users and objects

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