GRANT to Assign Privileges

by Sophia Tutorial

WHAT'S COVERED

This tutorial explores the GRANT and REVOKE commands to assign privileges on objects to roles in three parts:

1. Introduction
2. Possible Privileges
3. Examples

1. Introduction

When we create an object such as a table, view, or index, the object is assigned an owner. Typically, the owner of the object is the role that executed the CREATE statement associated with the object. For most types of objects, only the owner or superuser has the ability to do anything with the object. In order to allow other user or group roles to use and interact with the object, privileges on the object must be granted. There are many different types of privileges that are available to grant, depending on the type of object.

2. Possible Privileges

These privileges include:

- SELECT – Allows the role to select from any column or from specific columns listed within a table, view, or sequence. This privilege would also be required if there is a need to reference existing column values in an UPDATE or DELETE statement.
- INSERT – Allows the role to INSERT a new row within a table. If there are specific columns that are listed, only those columns may be inserted into the other columns automatically being set with default values.
- UPDATE – Allows the role to UPDATE a column or a list of columns in a table. If the UPDATE privilege is granted, the SELECT privilege should also be granted since it has to reference the table columns to determine which rows of data should be updated.
- DELETE – Allows the role to DELETE a row from a table. If the DELETE privilege is granted, the SELECT privilege should also be granted since it has to reference the table columns to determine which rows of data should be removed.
- ALL – This grants access to all available privileges to that object.

There are other privileges as well, including TRUNCATE, REFERENCES, TRIGGER, CREATE, CONNECT,

TEMPORARY, EXECUTE, and USAGE that allow interaction with objects.

3. Examples

Let us say we have a group role called employee_role. We may want to allow the querying of the employee table, but not allow any changes to the data. As such, we would run the following:

GRANT SELECT ON employee TO employee_role;
We could also grant the employee_role edit access and query access on the customer table:

GRANT SELECT, INSERT, UPDATE, DELETE ON customer TO employee_role;
As another example, for an admin_role, you could grant all privileges to the customer table:

GRANT ALL ON customer TO admin_role;
If we wanted to grant access to specific columns, we would add those columns in round brackets after the privilege type. For example, if we wanted to grant UPDATE privileges to the employee_role on the track table, but only on the unit_price, we would do the following:

GRANT UPDATE(unit_price) ON track TO employee_role;
This grants only the ability to update the price, but none of the other columns.

TRY IT

Your turn! Open the SQL tool by clicking on the LAUNCH DATABASE button below. Then enter in one of the examples above and see how it works. Next, try your own choices for which columns you want the query to provide.

SUMMARY

We can GRANT and REVOKE to assign and remove privileges to roles.

Source: Authored by Vincent Tran