Database Programming

Controlling User Access

ORACLE ACADEMY

Objectives

This lesson covers the following objectives:

- Compare the difference between object privileges and system privileges
- Construct the two commands required to enable a user to have access to a database
- Construct and execute a GRANT… ON …TO statement to assign privileges to objects in their schema to other users and/or PUBLIC
- Query the data dictionary to confirm privileges granted

Purpose

If you share a computer with others, whether at school or at home, you've probably had something you're working on or something you've saved either viewed, changed, or deleted by someone else. Wouldn't it be nice to be able to control the privileges others have to your personal files?

For databases, just as at school or home, data security is very important. In this lesson, you will learn how to grant or take away access to database objects as a means to control who can alter, delete, update, insert, index, or reference the database objects.

Controlling User Access

In a multiple-user environment, you want to maintain security of the database access and use. With Oracle Server database security, you can do the following:

- Control database access
- Give access to specific objects in the database
- Confirm given and received privileges within the Oracle data dictionary
- Create synonyms for database objects

Database Security

Database security can be classified into two categories:

- System security
- Data security

System security covers access and use of the database at the system level, such as creating users, usernames, and passwords, allocating disk space to users, and granting the system privileges that users can perform such as creating tables, views, and sequences. More than 100 distinct system privileges exist.

Database Security (cont.)

Data security (also known as object security) relates to object privileges which covers access to and use of the database objects, and the actions that those users can have on the objects. These privileges include being able to execute DML statements.

Privileges and Schemas

Privileges are the right to execute particular SQL statements. The DBA is a high-level user with the ability to grant users access to the database and its objects.

Users require system privileges to gain access to the database. They require object privileges to manipulate the content of the objects in the database.

Users can also be given the privilege to grant additional privileges to other users or to roles, which are named groups of related privileges.

Privileges and Schemas (cont.)

A schema is a collection of objects, such as tables, views, and sequences. The schema is owned by a database user and has the same name as that user.

In this course, your schema name is a combination of your country/state, school, course, and student number.

For example: uswa_skhs_sql01_s22

System Security

This level of security covers access and use of the database at the system level. More than 100 distinct system privileges exist.

System privileges such as the ability to create or remove users, remove tables, or backup tables are usually held only by the DBA.

System Security (cont.)

This table lists some of the system privileges which the DBA would not normally grant to other users. Would you want another user to be able to drop your tables?

System Privilege	Operations Authorized
CREATE USER	Grantee can create other Oracle users (a privilege required for a DBA role).
DROP USER	Grantee can drop another user.
DROP ANY TABLE	Grantee can drop a table in any schema.
BACKUP ANY TABLE	Grantee can backup any table in any schema with the export utility.
SELECT ANY TABLE	Grantee can query tables, views, or snapshots in any schema.
CREATE ANY TABLE	Grantee can create tables in any schema.

System Privileges

The DBA creates the user by executing the CREATE USER statement. The user does not have any privileges at this point. The DBA can then grant required privileges to that user.

```
CREATE USER user
IDENTIFIED BY   password;

CREATE USER  scott
IDENTIFIED BY ur35scott;
```

System Privileges (cont.)

Using the ALTER USER statement, a user can change their password.

```
ALTER USER scott
IDENTIFIED BY imscott35;
```

User System Privileges

The DBA uses the GRANT statement to allocate system privileges to the user. System privileges determine what the user can do at the database level. Once the user has been granted the privileges, the user can immediately use those privileges.

```
GRANT privilege [, privilege...]
TO user [, user| role, PUBLIC...];

GRANT  create session, create table, create sequence, create view
TO scott;
```

User System Privileges (cont.)

System Privilege	Operations Authorized
CREATE SESSION	Connect to the database.
CREATE TABLE	Create tables in the user's schema.
CREATE SEQUENCE	Create a sequence in the user's schema.
CREATE VIEW	Create a view in the user's schema.
CREATE PROCEDURE	Create a procedure, function, or package in the user's schema.

User System Privileges (cont.)

A user must have a CREATE SESSION privilege and a user id if he is to be able to access a database.

You cannot issue the CREATE SESSION command in Oracle Application Express; this happens automatically behind the scenes.

Object Security

This level of security covers access and use of the database objects and the actions users can have on those objects.

Object Privileges

Each object has a particular set of grantable privileges. The table below lists the privileges for various objects.

Object Privilege	Table	View	Sequence	Procedure
ALTER	X		X	
DELETE	X	X		
EXECUTE				X
INDEX	X	X		
INSERT	X	X		
REFERENCES	X			
SELECT	X	X	X	
UPDATE	X	X		

Object Privileges (cont.)

It is important to note the following four points regarding object privileges:

1. The only privileges that apply to a sequence are SELECT and ALTER. Remember, a sequence uses ALTER to change the INCREMENT, MAXVALUE, CACHE/NOCACHE, or CYCLE/NOCYCLE options. START WITH cannot be changed using ALTER.

Object Privileges (cont.)

2. You can grant UPDATE, REFERENCES, and INSERT privileges on individual columns in a table.

   For example:
   GRANT UPDATE (auth_expense)

   ON d_partners TO allison_plumb

3. A SELECT privilege can be restricted by creating a view with a subset of columns and granting the SELECT privilege only on the view. You can't grant SELECT on individual columns.

Object Privileges (cont.)

4. A privilege granted on a synonym is converted to a privilege on the base table referenced by the synonym. In other words, a synonym is simply a new, easier-to-use name. Using this name to grant a privilege is the same as granting the privilege on the table itself.

PUBLIC Keyword

An owner of a table can grant access to all users by using the PUBLIC keyword.

The example shown below allows all users on the system to query data from Alice’s DEPARTMENTS table.

```
GRANT select
ON alice.departments
TO PUBLIC;
```

The PUBLIC Keyword (cont.)

If a statement does not use the full name of an object, the Oracle server implicitly prefixes the object name with the current user's name (or schema). If user Scott queries the DEPARTMENTS table, for example, the system selects from the SCOTT.DEPARTMENTS table.

If a statement does not use the full name of an object, and the current user does not own an object of that name, the system prefixes the object name with PUBLIC.

The PUBLIC Keyword (cont.)

For example, if user Scott queries the USER_OBJECTS table, and Scott does not own such a table, the system selects from the data dictionary view by way of the PUBLIC.USER_OBJECTS public synonym.

Confirming Granted Privileges

If you attempt to perform an unauthorized operation, such as deleting a row from a table for which you do not have the DELETE privilege, the Oracle server does not permit the operation to take place.

If you receive the Oracle server error message “table or view does not exist,” you have done either of the following:

- Named a table or view that does not exist
- Attempted to perform an operation on a table or view for which you do not have the appropriate privilege.

View Privileges

You can access the data dictionary to view the privileges that you have. The chart shown describes various data dictionary views.

Using Oracle Application Express Developer, enter USER_ROLE_PRIVS, select the magnifying glass, then select any item to Query By Example. The user's privileges will be returned.

View Privileges (cont.)

Data Dictionary View	Description
ROLE_SYS_PRIVS	System privileges granted to roles
ROLE_TAB_PRIVS	Table privileges granted to roles
USER_ROLE_PRIVS	Roles accessible by the user
USER_TAB_PRIVS_MADE	Object privileges granted on the user’s objects
USER_TAB_PRIVS_RECD	Object privileges granted to the user
USER_COL_PRIVS_MADE	Object privileges granted on the columns of the user’s objects
USER_COL_PRIVS_RECD	Object privileges granted to the user on specific columns
USER_SYS_PRIVS	Lists system privileges granted to the user

Terminology

Key terms used in this lesson included:

- CREATE SESSION privilege
- Database link
- GRANT privilege
- Object privileges
- Object security
- Privilege
- PUBLIC privilege
- Role

Terminology (cont.)

Key terms used in this lesson included:

- Schema
- System privileges
- System security
- WITH GRANT OPTION

Summary

In this lesson, you should have learned how to:

- Compare the difference between object privileges and system privileges
- Construct the two commands required to enable a user to have access to a database
- Construct and execute a GRANT… ON …TO statement to assign privileges to objects in their schema to other users and/or PUBLIC
- Query the data dictionary to confirm privileges granted