

## EXERCISE-15

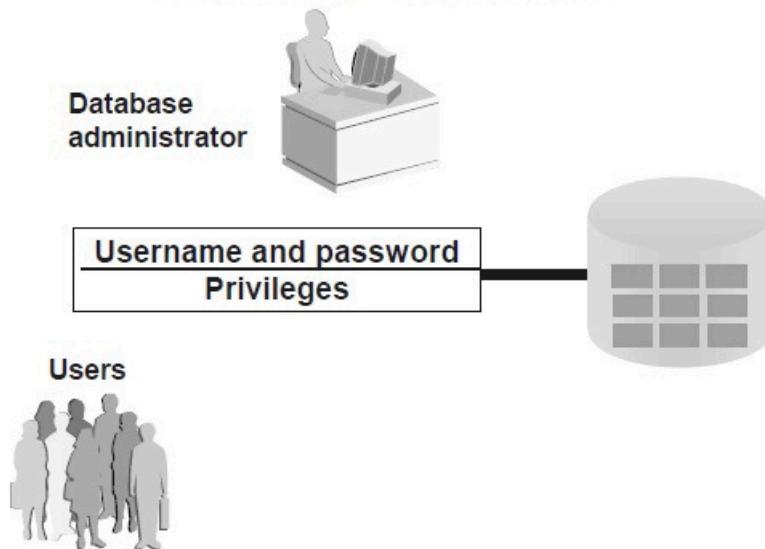
### Controlling User Access

#### Objectives

After the completion of this exercise, the students will be able to do the following:

- Create users
- Create roles to ease setup and maintenance of the security model
- Use the GRANT and REVOKE statements to grant and revoke object privileges
- Create and access database links

### **Controlling User Access**



#### 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* with the Oracle data dictionary
- Create synonyms for database objects

#### Privileges

- Database security:
  - System security
  - Data security
- System privileges: Gaining access to the database
- Object privileges: Manipulating the content of the database objects
- Schemas: Collections of objects, such as tables, views, and sequences

#### System Privileges

- level system privileges for tasks such as:
- Creating new users – Removing users
  - Removing tables – Backing up tables

#### **Typical DBA Privileges**

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 back up 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.

#### **Creating Users**

The DBA creates users by using the CREATE USER statement.

#### **EXAMPLE:**

CREATE USER scott IDENTIFIED BY tiger;

#### **User System Privileges**

- Once a user is created, the DBA can grant specific system privileges to a user.
  - An application developer, for example, may have the following system privileges:
    - CREATE SESSION
    - CREATE TABLE
    - CREATE SEQUENCE
    - CREATE VIEW
    - CREATE PROCEDURE
- GRANT *privilege* [, *privilege* ...]  
TO *user* [, *user|role*] *PUBLIC* ...];

#### **Typical User Privileges**

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 stored procedure, function, or package in the user's schema

#### **In the syntax:**

*privilege* is the system privilege to be granted

**Note:** Current system privileges can be found in the dictionary view SESSION\_PRIVS.

## **Granting System Privileges**

The DBA can grant a user specific system privileges.

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

### **What is a Role ?**

A role is a named group of related privileges that can be granted to the user. This method makes it easier to revoke and maintain privileges.

A user can have access to several roles, and several users can be assigned the same role. Roles are typically created for a database application.

### **Creating and Assigning a Role**

First, the DBA must create the role. Then the DBA can assign privileges to the role and users to the role.

---

```
CREATE ROLE role ;
```

In the syntax:

*role* is the name of the role to be created

Now that the role is created, the DBA can use the GRANT statement to assign users to the role as well as

**Syntax**  
assign privileges to the role.

### **Creating and Granting Privileges to a Role**

---

```
CREATE ROLE manager;
```

Role created.

```
GRANT create table, create view TO manager;
```

Grant succeeded.

```
GRANT manager TO DEHAAN, KOCHHAR;
```

Grant succeeded.

- Create a role

- Grant privileges to a role

- Grant a role to users

### **Changing Your Password**

- The DBA creates your user account and initializes your password.

---

## Object Privileges

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

### Object Privileges

- Object privileges vary from object to object.
- An owner has all the privileges on the object.
- An owner can give specific privileges on that owner's object.

GRANT *object\_priv* [(*columns*)]

ON *object*

TO {*user* |*role* |PUBLIC}

[WITH GRANT OPTION];

**In the syntax:**

*object\_priv* is an object privilege to be granted

ALL specifies all object privileges

*columns* specifies the column from a table or view on which privileges are granted

ON *object* is the object on which the privileges are granted

TO identifies to whom the privilege is granted

PUBLIC grants object privileges to all users

WITH GRANT OPTION allows the grantee to grant the object privileges to other users and roles

- Grant query privileges on the EMPLOYEES table.
- Grant privileges to update specific columns to users and roles. GRANT select ON employees TO sue, rich; GRANT update (department\_name, location\_id) ON departments TO scott, manager; **Using the WITH GRANT OPTION and PUBLIC Keywords**
- Give a user authority to pass along privileges.
- Allow all users on the system to query data from Alice's DEPARTMENTS table. GRANT select, insert ON departments TO scott WITH GRANT OPTION; . GRANT select ON alice.departments TO PUBLIC;

### How to Revoke Object Privileges

- You use the REVOKE statement to revoke privileges granted to other users.
- Privileges granted to others through the WITH GRANT OPTION clause are also revoked.
- REVOKE {privilege [, privilege...]|ALL} ON object FROM {user[, user...]|role|PUBLIC} [CASCADE CONSTRAINTS];

### In the syntax:

CASCADE is required to remove any referential integrity constraints made to the CONSTRAINTS object by means of the REFERENCES privilege

### Revoking Object Privileges the

---

As userAlice, revoke  
DEPARTMENTS  
table.

SELECT and INSERT privileges given to user Scott on the

FROM scott;

**Find the Solution for the following:**

1. What privilege should a user be given to log on to the Oracle Server? Is this a system or an object privilege?

To log on to the Oracle Server, a user must be granted the CREATE SESSION privilege. This is a system privilege allowing a user to establish a connection to the database and start a session.

---

2. What privilege should a user be given to create tables?

To create tables, a user must have the CREATE TABLE privilege, which is also a system privilege enabling the user to create new tables within their schema or database.

---

3. If you create a table, who can pass along privileges to other users on your table?

When you create a table, you as the owner have all privileges on that table, including the ability to grant (pass along) privileges to other users on your table. Only the owner or a user with special privileges can grant such object privileges.

4. You are the DBA. You are creating many users who require the same system privileges. What should you use to make your job easier?

As a DBA creating many users needing the same system privileges, you should create a role. A role is a named group of privileges that can be granted to many users, simplifying privilege management.

---

To change your Oracle user password, use the command:

```
ALTER USER your_username IDENTIFIED BY new_password;
```

6. Grant another user access to your DEPARTMENTS table. Have the user grant you query access to his or her DEPARTMENTS table.

```
GRANT SELECT ON your_schema.departments  
TO other_user WITH GRANT OPTION;
```

7. Query all the rows in your DEPARTMENTS table.

```
SELECT * FROM your_schema.departments;
```

8. Add a new row to your DEPARTMENTS table. Team 1 should add Education as department number 500. Team 2 should add Human Resources department number 510. Query the other team's table.

```
INSERT INTO departments (department_id, department_name)      1 row inserted.  
VALUES (500, 'Education');                                Elapsed: 00:00:00.005  
  
INSERT INTO departments (department_id, department_name)      1 row inserted.  
VALUES (510, 'Human Resources');                           Elapsed: 00:00:00.001
```

9. Query the USER\_TABLES data dictionary to see information about the tables that you own.

```
SELECT * FROM other_team_schema.department;
```

10. Revoke the SELECT privilege on your table from the other team.

```
REVOKE SELECT ON your_schema.departments  
FROM other_user;
```

11. Remove the row you inserted into the DEPARTMENTS table in step 8 and save the changes.

```
DELETE FROM departments WHERE department_id = 500;  
COMMIT;
```

Commit complete.

Elapsed: 00:00:00.001

<u>Evaluation Procedure</u>	<u>Marks awarded</u>
<u>Practice Evaluation (5)</u>	
<u>Viva(5)</u>	
<u>Total (10)</u>	
<u>Faculty Signature</u>	