14

Controlling User Access

ORACLE®

Objectives

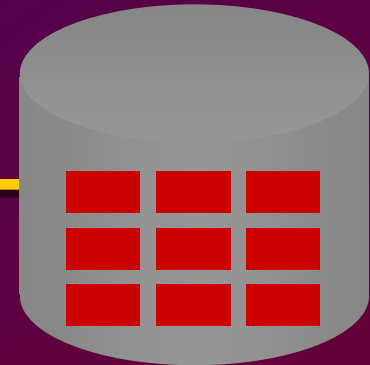**After completing this lesson, you should be able to do the following:**

- **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**

ORACLE®

Controlling User Access

Database administrator

Username and password privileges

Users

ORACLE®

Privileges

- **Database security:**
    - **System security**
    - **Data security**

- **System privileges: Gain access to the database**

- **Object privileges: Manipulate the content of the database objects**

- **Schema: Collection of objects, such as tables, views, and sequences**

ORACLE®

System Privileges

- **More than 80 privileges are available.**
- **The DBA has high-level system privileges:**
  - **Create new users**
  - **Remove users**
  - **Remove tables**
  - **Back up tables**

ORACLE®

Creating Users

The DBA creates users by using the CREATE USER statement.

```
CREATE USER      user
IDENTIFIED BY   password;
```

```
SQL> CREATE   USER   scott
  2   IDENTIFIED BY tiger;
User created.
```

ORACLE®

User System Privileges

- **Once a user is created, the DBA can grant specific system privileges to a user.**

```
GRANT privilege [, privilege...]
TO user [, user...];
```

- **An application developer may have the following system privileges:**
  - **CREATE SESSION**
  - **CREATE TABLE**
  - **CREATE SEQUENCE**
  - **CREATE VIEW**
  - **CREATE PROCEDURE**

ORACLE®

Granting System Privileges

The DBA can grant a user specific system privileges.

```
SQL> GRANT   create table, create sequence, create view
  2  TO      scott;
Grant succeeded.
```
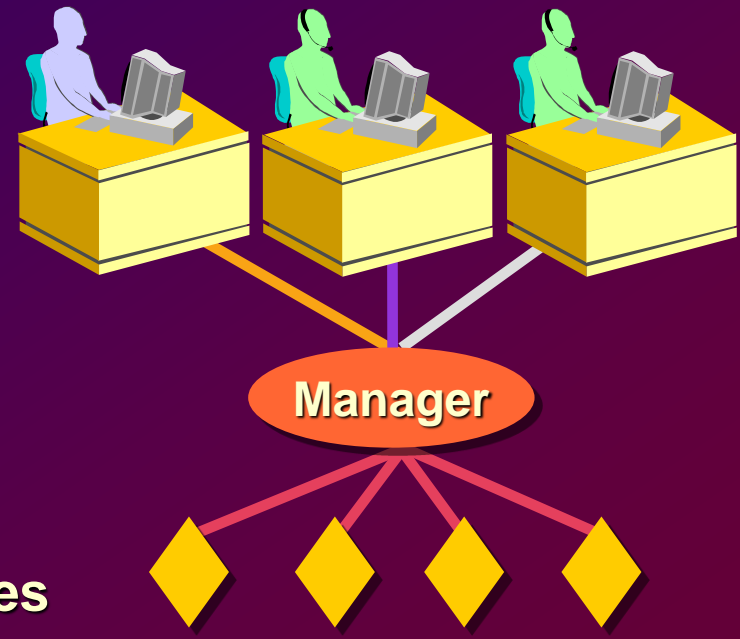
ORACLE®

What Is a Role?
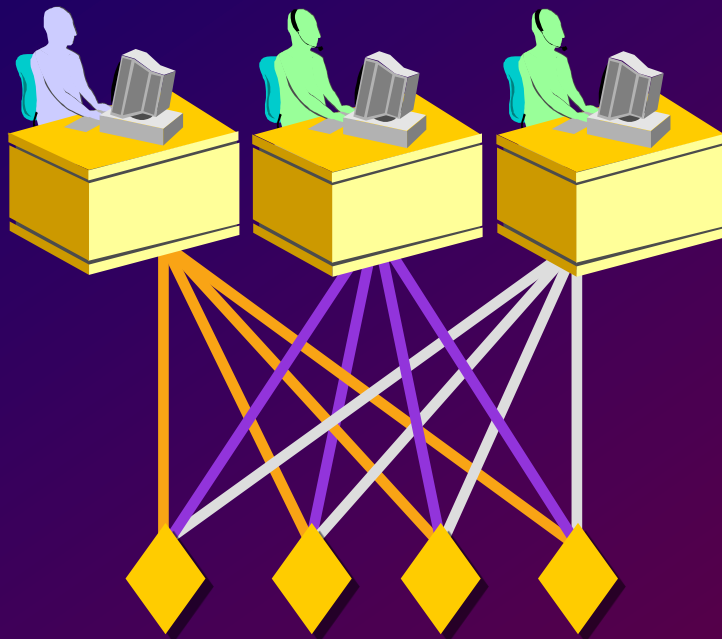
Users

Privileges

Allocating privileges without a role

Allocating privileges with a role

Manager

ORACLE®

Creating and Granting Privileges to a Role

```
SQL> CREATE ROLE manager;
Role created.
```

```
SQL> GRANT create table, create view
  2        to manager;
Grant succeeded.
```

```
SQL> GRANT manager to BLAKE, CLARK;
Grant succeeded.
```

ORACLE®

Changing Your Password

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

- **You can change your password by using the ALTER USER statement.**

```
SQL> ALTER USER scott
  2        IDENTIFIED BY lion;
User altered.
```

ORACLE®

Object Privileges

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

ORACLE®

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];
```

ORACLE®

Granting Object Privileges

- **Grant query privileges on the EMP table.**

```
SQL> GRANT     select
  2  ON        emp
  3  TO        sue, rich;
Grant succeeded.
```

- **Grant privileges to update specific columns to users and roles.**

```
SQL> GRANT     update (dname, loc)
  2  ON        dept
  3  TO        scott, manager;
Grant succeeded.
```

ORACLE®

Using WITH GRANT OPTION and PUBLIC Keywords

- **Give a user authority to pass along the privileges.**

```
SQL> GRANT    select, insert
  2  ON       dept
  3  TO       scott
  4  WITH GRANT OPTION;
Grant succeeded.
```

- **Allow all users on the system to query data from Alice's DEPT table.**

```
SQL> GRANT    select
  2  ON       alice.dept
  3  TO       PUBLIC;
Grant succeeded.
```

ORACLE®

Confirming Privileges Granted

Data Dictionary Table	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

ORACLE®

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 will also be revoked.**

```
REVOKE  {privilege [, privilege...]|ALL}
ON      object
FROM    {user[, user...]|role|PUBLIC}
[CASCADE CONSTRAINTS];
```

ORACLE®

Revoking Object Privileges

As user Alice, revoke the SELECT and INSERT privileges given to user Scott on the DEPT table.

```
SQL>  REVOKE    select, insert
  2   ON        dept
  3   FROM      scott;
Revoke succeeded.
```

ORACLE®

Summary

Statement	Action
CREATE USER	Allows the DBA to create a user
GRANT	Allows the user to give other users privileges to access the user's objects
CREATE ROLE	Allows the DBA to create a collection of privileges
ALTER USER	Allows users to change their password
REVOKE	Removes privileges on an object from users

ORACLE®

Practice Overview

- **Granting other users privileges to your table**

- **Modifying another user's table through the privileges granted to you**

- **Creating a synonym**

- **Querying the data dictionary views related to privileges**

ORACLE®