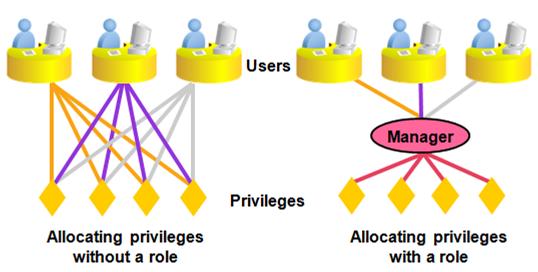
**INT207 Lab 5**

## Roles

***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.



## Note: Role and username must be a unique name.

## Creating and Assigning a Role

## First, the DBA must create the role. Then the DBA can assign privileges to the role and assign the role to users. There are 3 steps to implement a role.

## Create a role

**CREATE ROLE *role\_name ;***

## Assign privileges to the role: A role can consist of both system and object privileges.

***System Privileges***

**GRANT system\_priv1 [, system\_priv2,…]**

**TO *role\_name* ;**

***Object Privileges***

**GRANT object\_priv1,[ object\_priv2, …]**

**ON [schema.]object\_name**

**TO *role\_name* ;**

**Question:** Give at least 3 system privileges and 3 object privileges.

## Assign the role to users: Roles can be granted to and revoked from users or other roles

**GRANT role1 [,role2, …]**

**TO *user* [WITH ADMIN OPTION] *|role*;**

**REVOKE role1 [,role2, …]**

**FROM *user |role* ;**

**Note:** *Role does NOT affect current sessions.*

**Example:** 1. CREATE ROLE manager;

*Role created.*

2. GRANT select,update,delete on student TO manager;

*Grant succeeded.*

3. GRANT manager TO scott, bob;

*Grant succeeded.*

# Confirming Granted Roles from Data Dictionary Views:

You can access the data dictionary view named ***USER\_ROLE\_PRIVS*** to view the roles accessible by the user

SQL> SELECT \* FROM user\_role\_privs ;

**Dropping a role**

Only the database owner can drop a role. To drop a role, use the DROP ROLE statement.

Dropping a role effectively revokes all grants of this role to users and other roles.

**DROP ROLE *role\_name ;***

**Data Dictionary**

|  |  |
| --- | --- |
| Data Dictionary | Description |
| USER\_SYS\_PRIVS | List system privileges granted to the current user |
| USER\_TAB\_PRIVS | List object privileges granted to the current user |
| USER\_TAB\_PRIVS\_MADE | List grants on all objects owned by the current user |
| USER\_TAB\_PRIVS\_RECD | List objects grants for which the current user is the grantee |
| USER\_ROLE\_PRIVS | List roles granted to the current user |
| ROLE\_SYS\_PRIVS | List system privileges granted to roles that the user has access |
| ROLE\_TAB\_PRIVS | List object privileges granted to roles that the user has access |
| DBA\_ROLES | List all roles that exist in the database |

**References**

http://docs.oracle.com/cd/B19306\_01/network.102/b14266/admusers.htm#i1008437

***Task 1:* *Using Roles***

**Connect the database as user <DBxxxx>**

|  |
| --- |
| Revoke all object privileges on PHONELIST from the user <APPxxxx> . \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Create a role named R\_DEVxxxx and grant the SELECT and UPDATE privileges on the PHONELIST table to the R\_DEVxxxx role. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Create a role named R\_MGRxxxx and grant the INSERT and DELETE privileges on the PHONELIST table to the R\_MGRxxxx role. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Grant the role R\_DEVxxxx to the R\_MGRxxxx role. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Grant the R\_DEVxxxx role to user <APPxxxx> that can be passed the granted role to other users and roles. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Connect the database as user <APPxxxx>**

**Note: *If you do Lab 3 completely, the password of a user <APPxxxx> will be <dbms>.***

|  |
| --- |
| Verify the granted role by checking data from data dictionary views. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Now, Can user <APPxxxx> select all columns of DBxxxx.PHONELIST table? [Y|N] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Connect the database as user <DBxxxx>**

|  |
| --- |
| Revoke the R\_DEVxxxx role from user <APPxxxx> and grant the R\_MGRxxxx role to user <APPxxxx>. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Connect the database as user <APPxxxx>**

|  |
| --- |
| Verify the granted role by checking data from data dictionary view. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Now, Can user <APPxxxx> delete a row of DBxxxx.PHONELIST table? [Y|N] *Hint: If you can delete it, please rollback the deletion.*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Connect the database as user <DBxxxx>**

|  |
| --- |
| Revoke ONLY the UPDATE privilege from the R\_DEVxxxx role.How does this revoke effects to the user <APPxxxx>? Please verify \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ User <DBxxxx> wants to limit the role R\_DEVxxxx to update data ONLY column PHONE\_NUMBER of the DBxxxx.PHONELIST table.How does user <DBxxxx> do for supporting the requirement? Please do it. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_     1. Remove the R\_MGRxxxx role.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   1. Verify that the role R\_MGRxxxx is removed.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_