Administering Users for Security Purposes

Welcome to the third module of this course. For this lesson, we will discuss the importance of administering user and assign a specific role.

It is important to plan how many Users will have an access to the database, what specific privileges should be given on each users and how to revoke a privilege.

User and Roles

A user **privilege** is a right to execute a particular type of SQL statement, or a right to access another user's object. The types of privileges are defined by Oracle.

Roles, on the other hand, are created by users (usually administrators) and are used to group together privileges or other roles. They are a means of facilitating the granting of multiple privileges or roles to users.

After completing this lesson, the student should be able to:

- Identify how to control user access.
- Define what the difference between a user and a role is.
- Define and enumerate the two type of privilege.
- Create a new USER
- Grant Privilege access to a specific User.
- Changes password
- Create and Grant role
- Pass Privileges
- Revoke Privileges
-

Database User Accounts

- Each database user account has:
  - A unique username
  - An authentication method
  - A default tablespace

  - A temporary tablespace
  - A user profile
  - An initial consumer group
  - An account status
- A schema:
  - Is a collection of database objects that are owned by a database user
  - Has the same name as the user account

Predefined Administrative Accounts

- Operating system security:
  - DBAs must have the OS privileges to create and delete files.
  - Typical database users should not have the OS privileges to create or delete database files.
- Administrator security:
  - For SYSDBA, SYSOPER, and SYSASM connections:
    - DBA user by name is audited for password file and strong authentication methods
    - OS account name is audited for OS authentication
    - OS authentication takes precedence over password file authentication for privileged users
    - Password file uses case-sensitive passwords

Privileges

- There are two types of user privileges:
  - System: Enables users to perform particular actions in the database
  - Object: Enables users to access and manipulate a specific object

Benefits of Roles

- Easier privilege management
- Dynamic privilege management
- Selective availability of privileges

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
- Database security can be classified into two categories: system security and data security.
    - System security covers access and use of the database at the system level such as the username and password, the disk space allocated to users, and the system operations that users can perform.
    - Database security covers access and use of the database objects and the actions that those users can have on the 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: Collection of objects such as tables, views, and sequences

System Privileges

- More than 100 privileges are available.
- The database administrator has high-level system privileges for tasks such as:

- Creating new users
- Removing users
- Removing tables
- Backing up tables

Creating Users

- The DBA creates users with the CREATE USER statement.
- Syntax:

```
CREATE USER user_name
IDENTIFIED BY user_password;
```

- **Example:**

```
Create USER IT_MGR
Identified by itmanager;
```

- The given example will create a user named as IT_MGR with a predefine password set as itmanager.
- This user IT_MGR may access only the oracle server once a session is granted. A session in database is also known as system privilege.

User System Privileges

- After a user is created, the DBA can grant specific system privileges to that user.
- Syntax:

```
GRANT PRIVILEGE [privilege_type….]
TO user_name [,user| role, PUBLIC…];
```

- Example:

```
GRANT CREATE SESSION
TO IT_MGR;
```

- In the given example the user IT_MGR will now have the privilege to access the oracle sever because of CREATE SESSION privilege granted to him.
- This means this user can now start initiating a connection to the server.
- An application developer, for example, may have the following system privileges:

- CREATE SESSION
- CREATE TABLE
- CREATE SEQUENCE
- CREATE VIEW
- CREATE PROCEDURE

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 assign the role to users.

  - In order for the user let say IT_MGR after establishing a session in oracle server perform DML, DDL and SELECT operation a role must be created first and must be granted to a certain user.

  - **Syntax**

    CREATE ROLE *role*;

  - In the syntax:

    role is the name of the role to be created

  - Example:

    CREATE role IT;

  - After the role is created, the DBA can use the GRANT statement to assign the role to users as well as assign privileges to the role.

  - Note that: make sure that before you grant a role to a certain user a specific object privileges must be

associated so that a user can user the role assigned to him.

Changing Your Password

- The DBA creates your user account and initializes your password.
- You can change your password by using the ALTER USER
- Although a password is defined during the creation of user at system level a user may also change the defined password assigned to them.
- Example:

  ALTER USER IT_MGR
  Identified by myownpassword01;
  - Since a new password is changed user IT_MGR will have to used it whenever he establishes a connection in oracle server.
  - The user IT_MGR will now have the new password set as myornpassword01.

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.
- For the role example IT to have access in system object a privilege must be granted.
- Syntax:

  GRANT object_priv [(columns)]
  ON object
  TO {user|role|PUBLIC}
  [WITH GRANT OPTION];
- **Example:**

GRANT SELECT, INSERT, UPDATE, DELETE
ON EMPLOYEES
TO IT;

- In this example the role IT will now have an object privilege such as SELECT statement, DML (INSERT, UPDATE and DELETE) to the object EMPLOYEES, which only means that IT can perform this statement into the table EMPLOYEES even if his global connection in thru the SYSTEM.

- Since this role cannot establish a connection in the server, this must be granted to a user. Using the example below:

GRANT IT
To IT_MGR

- all the associated role of IT is now granted to IT_MGR, this means IT_MGR can now perform SELECT, INSERT , UPDATE and DELETE

Passing on your Privileges

- Give a user authority to pass along privileges as shown in the example below:

- A privilege that is granted with the WITH GRANT OPTION clause can be passed on to other users and roles by the grantee. Object privileges granted with the WITH GRANT OPTION clause are revoked when the grantor's privilege is revoked.

```
SQL> GRANT SELECT, INSERT
  2  ON EMPLOYEES
  3  TO tiger
  4  WITH GRANT OPTION;

Grant succeeded.
```

- The example on the slide gives user TIGER access to EMPLOYEES table with the privileges to query the table and add rows to the table. The example also shows that TIGER can give others these privileges.

Revoking other 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.

- Example:

```
SQL> REVOKE SELECT, INSERT
  2  ON SYSTEM.EMPLOYEES
  3  FROM IT_MGR;

Revoke succeeded.
```

LESSON SUMMARY:

In this lesson, you should have learned about statements that control access to the database and database objects.

- Create new user using **CREATE USER** user and is usually performed by the Database Admin
- Grant specific privileges either Private or Public using the **GRANT** option.
- Create specific privileges by using the **CREATE ROLE**
- Change password created by using the **ALTER USER** statement
- Removes privileges on an object by using the **REVOKE** statement

Activities/Exercises

- Download the Laboratory Exercise 1: Managing User and Roles in LMS Portal.
- Download the Departments.txt – this is the table to use for the succeeding activity
- Follow the instruction carefully, when you skip once transaction that must be performed before jumping unto the next number this might cause a different output.
- In each number questions with essay part should answered briefly, question with PL/SQL requires the PL/SQL used in order to come up with the solution.

Glossary

- **Database security** covers access and use of the database objects and the actions that those users can have on the objects.
- **DBSNMP account** - is granted the OEM_MONITOR role
- **Object:** Enables users to access and manipulate a specific object
- **Object privileges:** Manipulating the content of the database objects
- **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.
- **Schema** – is a collection of database objects that are owned by a database user
- **System:** Enables users to perform particular actions in the database
- **SYSTEM account** - is granted the DBA, MGMT_USER, and AQ_ADMINISTRATOR_ROLE roles.
- **System privileges:** Gaining access to the database
- **System security** - covers access and use of the database at the system level such as the username and password, the disk space allocated to users, and the system operations that users can perform.
- **SYS account -** is granted the DBA role, as well as several other roles.
- **SYSMAN account** - is granted the MGMT_USER, RESOURCE and SELECT_CATALOG_ROLE roles.

References

Textbook:

- Oracle Database 11g 2nd Edition K Gopalakrishnan (2012)

References:

- Carlos, Peter (2009). Database Systems
- Connoly, Thomas & Begg, Carolyn (2010). Database Systems : A practical approach to design, implementation and management
- Sciore, Edward (2009). Database Design and Implementation
- Bulusu, Lakshman (2008). Oracle PL/SQL : Expert Techniques for Developers and Database Administrators
- Loshin, David (2008). Master Data Management

Other Suggested Readings (e.g. periodicals, articles, websites, IT applications/software, etc.):

- www.oracle.com
- www.apex.oracle.com
- SQL Tutorial. In ws3schools, Retrieved from http://www.w3schools.com/sql/default.asp
- SQL. In Encyclopedia Britannica, Retrieved from http://www.britannica.com/EBchecked/topic/569684/SQL
- Database Administration. In Encyclopedia.com, Retrieved from http://www.encyclopedia.com/topic/Database_administration.aspx
- SQL. In Encyclopedia.com, Retrieved from http://www.encyclopedia.com/topic/SQL.aspxLearning Icons