

Módulo: Bases de Datos

Unidad 3: Bases de Datos Relacionales

Sesión 4: DCL: Usuarios, roles y privilegios

Descripción:

En la presente unidad hemos estudiado los distintos mecanismos de control de acceso que tiene Oracle en base a la definición de usuarios, privilegios y roles. Aprovecharemos esta sesión para practicar desde el SQL Plus (consola de acceso al SGBD Oracle usando comandos). Para practicar todos estos conceptos se pide.

- Crear un usuario llamado “paradoc1” con password “oracle1”.
- Crear un usuario llamado “paradoc2” con password “oracle2”.
- Conceder al usuario llamado “paradoc1” la capacidad para poder realizar consultas sobre una tabla concreta del sistema.
- Intenta realizar la consulta sobre dicha tabla del sistema.
- Revocar el privilegio de consulta otorgado a paradoc1 y volver a intentar a realizar la consulta.
- Conceder los privilegios a paradoc2 para realizar inserciones sobre las columnas department_id y department_name de la tabla departments.
- Conceder los privilegios a paradoc2 para realizar actualizaciones sobre las columnas department_id y department_name de la tabla departments.
- Probar que la concesiones de privilegios concretos sobre las columnas funcionan.
- Conceder el privilegio de sistema para consultar cualquier tabla al usuario paradoc1.
- Crear un rol llamado “consulta”
- Crear un rol llamado “modificación”
- Conceder a “consulta” privilegios de consultar información de cualquier tabla.
- Conceder a “modificación” privilegios de modificación sobre cualquier tabla.
- Conceder a “paradoc1” el rol de “consulta”.
- Conceder a “paradoc2” el rol de “modificación”.

Criterios de Evaluación:

- RA2_g: Se han creado los usuarios y se les han asignado privilegios.
- RA2_h: Se han utilizado asistentes, herramientas gráficas y los lenguajes de definición y control de datos.

Objetivos:

- Conocer los conceptos de usuario, rol y privilegio.
- Crear, editar y eliminar un usuario.
- Crear y asignar roles.
- Otorgar y revocar privilegios a un usuario o a un rol.

Recursos:

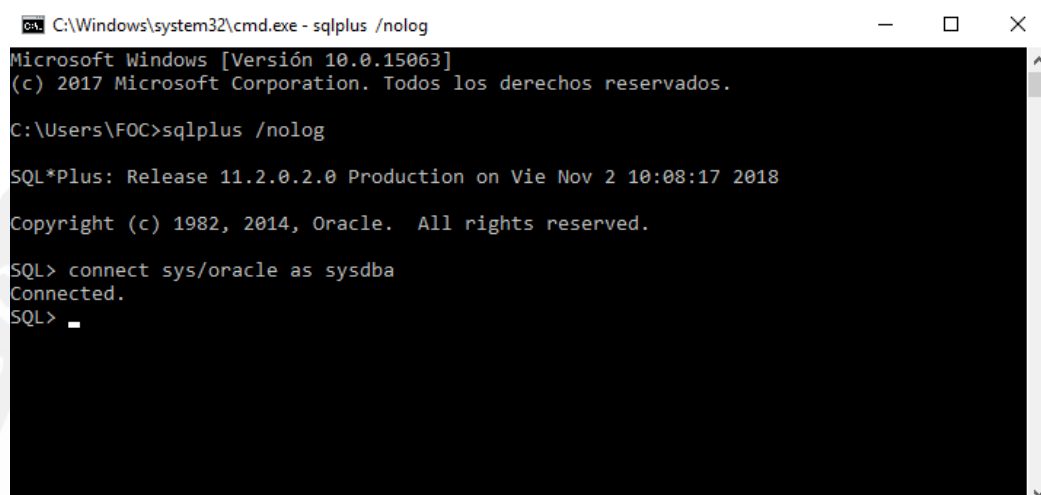
- Acceso a Internet.
- Procesador de Textos.
- Oracle Express Edition.
- SQL Plus.

Conceptos a revisar previamente:

- Realizar el estudio de los apartados:
 - Usuarios. Roles. Privilegios. Objetos
 - Lenguaje de control de datos (DCL). Herramientas gráficas proporcionadas por el sistema gestor para la definición de usuarios, roles y privilegios.
- Realizar el ejercicio resuelto:
 - "Creación de Usuario, Roles y privilegios "
- Ver video conceptos:
 - "Privilegios"
 - "Roles"

Resolución de la práctica:

Para conectarnos a Oracle por medio de SQLPlus, tenemos que abrir una consola de Windows poniendo el comando 'cmd' en "Ejecutar". Una vez tengamos la terminal deberemos ejecutar los comandos que se ven en la imagen "Conectar con Oracle con SQLPlus".



```
C:\Windows\system32\cmd.exe - sqlplus /nolog
Microsoft Windows [Versión 10.0.15063]
(c) 2017 Microsoft Corporation. Todos los derechos reservados.

C:\Users\FOC>sqlplus /nolog

SQL*Plus: Release 11.2.0.2.0 Production on Vie Nov 2 10:08:17 2018

Copyright (c) 1982, 2014, Oracle. All rights reserved.

SQL> connect sys/oracle as sysdba
Connected.
SQL>
```

Imagen: Conectar con Oracle con SQLPlus

El comando 'sqlplus /nolog' nos permite conectarnos al SGBD sin conectarnos con un usuario concreto. Para conectarnos con un usuario la sintaxis sería:

```
CONNECT usuario/password [as ROL]
```

Para conectarnos con el usuario 'sys' con el rol 'sysdba', como lo hacemos en SQLDeveloper, tenemos que:

```
CONNECT sys/oracle as sysdba
```

Nota: En las bases de datos multiusuario Oracle cuando hacemos algunas tareas internas con los usuarios del sistema nos puede dar problemas y darnos el siguiente mensaje de error "error.: ORA-65096: invalid common user or role name in Oracle".

La forma de solucionar este error es utilizar el prefijo C## o c##. Pero si queremos trabajar con normalidad tenemos también el parámetro _ORACLE_SCRIPT que nos ayuda a anular este error.

Para modificar este parámetro hay que hacerlo de la siguiente manera:

```
ALTER SESSION SET "_oracle_script" = true;
```

- Crear un usuario llamado "paradoc1" con password "oracle1"

```
CREATE USER paradoc1 IDENTIFIED BY "oracle1";  
Connect paradoc1/oracle1 -> no funciona ya que no tenemos  
permiso de crear sesión
```

```
GRANT CREATE SESSION TO paradoc1;  
Connect paradoc1/oracle1 -> Ya si funciona
```

- Crear un usuario llamado "paradoc2" con password "oracle2"

```
CREATE USER paradoc2 IDENTIFIED BY "oracle2";
```

- Conceder al usuario llamado "paradoc1" la capacidad para poder realizar consultas sobre una tabla concreta del sistema.

```
Select * from HR.Departments; -> desde SYS y desde paradoc1  
GRANT SELECT ON HR.departments TO paradoc1;
```

- Intenta realizar la consulta sobre dicha tabla del sistema.

```
Select * from HR.Departments;
```

- Revocar el privilegio de consulta otorgado a paradoc1 y volver a intentar a realizar la consulta.

```
REVOKE SELECT ON HR.Departments FROM paradoc1;
```

- Conceder los privilegios a paradoc2 para realizar inserciones sobre las columnas department_id y department_name de la tabla departments.

```
GRANT INSERT (department_id, department_name) ON  
HR.Departments TO paradoc2;
```

- Conceder los privilegios a paradoc2 para realizar actualizaciones sobre las columnas department_id y department_name de la tabla departments.

```
GRANT UPDATE (department_id, department_name) ON  
HR.Departments TO paradoc2;
```

- Probar que las concesiones de privilegios concretos sobre las columnas funcionan.

```
INSERT INTO HR.departments (department_id,  
department_name) values (500, 'mi_depar');
```

```
INSERT INTO HR.departments (department_id,  
department_name,manager_id) values (500, 'mi  
depar',101); -> no me dejaria
```

```
UPDATE HR.departments SET department_name=  
'depar_FOC' where department_id=500;
```

```
UPDATE HR.departments SET manager_id = 102 WHERE  
department_id=500; -> no me deja
```

- Conceder el privilegio de sistema para consultar cualquier tabla al usuario paradoc1.

```
GRANT SELECT ANY TABLE TO paradoc1;
```

- Crear un rol llamado "consulta"

```
CREATE ROLE consulta;
```

- Crear un rol llamado "modificación"

```
CREATE ROLE modificacion;
```

- Conceder a "consulta" privilegios de consultar información de cualquier tabla del sistema.

```
GRANT SELECT ANY TABLE TO consulta;
```

- Conceder a "modificación" privilegios de modificación sobre cualquier tabla del sistema.

```
GRANT UPDATE ANY TABLE TO modificacion;
```

- Conceder a "paradoc1" el rol de "consulta"

```
GRANT consulta TO paradoc1;
```

- Conceder a "paradoc2" el rol de "modificación"

```
GRANT modificacion TO paradoc2;
```