

Título	
PRÁCTICA SEGURIDAD ORACLE	
Finalidad	Autor
Práctica guiada sobre configuración de seguridad en Oracle.	Eduardo Encalada aeencalada@utpl.edu.ec
	Revisión
	Sep-2021

Introducción

Para complementar la explicación acerca del control de acceso lógico que debe existir en la implementación de una base de datos, presentamos aquí una práctica que muestra cómo crear usuarios y asignar permisos en Oracle.

Para comprender más en detalle los comandos Oracle requeridos, revisar la documentación Oracle referente al Lenguaje de control de datos (DCL por sus siglas en inglés), específicamente el tema "[Administering User Privileges, Roles, and Profiles](#)".

Software requerido:

- [Oracle Database Express Edition \(XE\) 11g](#)
- [SQL Developer](#)

Escenario:

Para nuestro ejemplo vamos a aprovechar el esquema de datos **HR** (Human Resources) que ya viene precargado cuando instalamos Oracle XE 11g. En este caso el propietario de ese esquema es el usuario HR, y por tanto tiene acceso y permisos a los objetos allí almacenados.

En Oracle además existen otros usuarios (superusuarios) que pueden acceder de forma ilimitada a todos los objetos de todos los esquemas de la base de datos, son aquellos usuarios que tienen asignado el rol DBA. Inicialmente al instalar la Oracle existen dos usuarios con ese rol: SYS y SYSTEM. Luego se pueden crear otros usuarios con rol DBA, que es recomendable solo para usuarios administradores.

Lo que buscamos con esta práctica es:

- Crear nuevos usuarios
- Asignar permisos a esos nuevos usuarios para que puedan conectarse a la base de datos y acceder a los objetos de HR
- Crear roles
- Asignar privilegios a roles
- Asignar roles a usuarios

Pasos iniciales.

Para la práctica usaremos la herramienta SQL Developer.

1. Abrir una sesión como usuario SYS
2. Desbloquear usuario HR:

```
ALTER USER "HR" ACCOUNT UNLOCK;
```

3. Establecer un nuevo password para usuario HR:

```
ALTER USER "HR" IDENTIFIED BY "oracle";
```

4. Abrir una nueva sesión como usuario HR

5. Verificar que podemos navegar por todos los objetos de HR

PRÁCTICA

Creación de usuarios:

Cuando creamos un usuario en Oracle, éste no tiene asignado ningún privilegio de acceso, por lo tanto, aunque las credenciales del usuario existan, no podrá acceder aun a la base de datos, ni tan siquiera abrir una sesión Oracle.

La creación de nuevos usuarios únicamente lo puede realizar un usuario con rol DBA

1. Como SYS: crear un nuevo usuario “INVITADO” con password “pwdinvitado”

```
CREATE USER invitado IDENTIFIED BY pwdinvitado;
```

2. Probar si se puede abrir una sesión con el usuario creado. Desde SQL Developer crear una nueva conexión para el usuario creado y probar si funciona.

El resultado es:

```
Status : Failure -Test failed: ORA-01045: user INVITADO lacks CREATE  
SESSION privilege; logon denied
```

Como vemos nos indica que no se permite el acceso porque no tiene permiso CREATE SESSION.

Siempre que creamos un usuario debemos también asignarle dos ROLES básicos: CONNECT y RESOURCE. El rol CONNECT agrupa todos los privilegios necesarios para abrir una sesión oracle y RESOURCE contiene todos los privilegios para crear y administrar objetos dentro del esquema asociado al usuario (en este caso el esquema INVITADO)

3. Como SYS: asignar roles CONNECT y RESOURCE al usuario INVITADO.

```
GRANT CONNECT,RESOURCE TO INVITADO;
```

4. Probar si ahora ya se puede abrir una sesión con el usuario creado.

```
Status: Success
```

En efecto ahora INVITADO ya puede acceder a la base de datos Oracle.

En este punto INVITADO solo podrá acceder a objetos que le pertenezcan, es decir objetos que estén en su esquema (INVITADO). Lo verificamos:

5. Como usuario INVITADO: probar si INVITADO puede acceder a consultar la tabla JOBS del esquema HR

```
SELECT * FROM HR.JOBS;
```

```
SQL Error: ORA-00942: table or view does not exist
00942. 00000 - "table or view does not exist"
```

Nos indica que la tabla o vista que se intenta consultar NO EXISTE. Pero la tabla JOBS si existe en HR, el problema es que INVITADO no tiene aún ningún permiso para accederla y por lo tanto no la puede ver.

Asignación de permisos para acceder a objetos de otros esquemas

En Oracle, si queremos que un usuario que NO tiene rol DBA acceda a los objetos de un esquema que no es el propio, se le debe asignar permisos de forma explícita.

Los permisos sobre objetos de un esquema X los puede asignar el usuario dueño del esquema X o cualquier usuario con rol DBA.

Nota: Cuando se accede a otro esquema distinto al del usuario con el cual se encuentra logueado, siempre debe anteponerse para cada tabla el nombre del esquema seguido de punto (cualificar el nombre de las tablas)

6. Al usuario INVITADO otorgarle permiso para que pueda acceder a la tabla JOBS de HR, únicamente para realizar consultas. Para ello como SYS o como HR, ejecutar:

```
GRANT SELECT ON HR.JOBS TO INVITADO;
```

7. Como usuario INVITADO: probar si INVITADO puede acceder a consultar la tabla JOBS del esquema HR

```
SELECT * FROM HR.JOBS;
```

JOB_ID	JOB_TITLE	MIN_SALARY	MAX_SALARY
AD_PRES	President	20080	40000
AD_VP	Administration Vice President	15000	30000
.	.	.	.
.	.	.	.

19 rows selected

```
SELECT COUNT(*) FROM HR.JOBS;
```

COUNT(*)
19

8. A usuario INVITADO otorgarle permisos para que pueda consultar y agregar nuevos registros a la tabla REGIONS de HR. Como usuario SYS o como HR ejecutar:

```
GRANT SELECT, INSERT ON HR.REGIONS TO INVITADO;
```

9. Como usuario INVITADO, probar se puede consultar la tabla HR.REGIONS

```
SELECT MAX(REGION_ID) FROM HR.REGIONS;
```

MAX(REGION_ID)
19

10. Como usuario INVITADO, probar se puede insertar en la tabla HR.REGIONS. Para ello agregaremos una nueva región “Oceanía” con ID 5.

```
INSERT INTO HR.REGIONS VALUES (5, 'Oceania');
```

```
1 rows inserted.
```

11. Revocar a INVITADO el permiso de inserción en la tabla REGIONS de HR. Como usuario SYS o HR ejecutar:

```
REVOKE INSERT ON HR.REGIONS FROM INVITADO;
```

12. Nuevamente como usuario INVITADO, probar lo anterior tratando de insertar una nueva región:

```
INSERT INTO HR.REGIONS VALUES (6, 'Africa');
```

```
SQL Error: ORA-01031: insufficient privileges  
01031. 00000 - "insufficient privileges"
```

***Cause:** An attempt was made to change the current username or password without the appropriate privilege. This error also occurs if attempting to install a database without the necessary operating system privileges.
When Trusted Oracle is configured in DBMS MAC, this error may occur if the user was granted the necessary privilege at a higher label than the current login.

***Action:** Ask the database administrator to perform the operation or grant the required privileges.
For Trusted Oracle users getting this error although granted the the appropriate privilege at a higher label, ask the database administrator to regrant the privilege at the appropriate label.

13. Igualmente, como usuario INVITADO, probar que tampoco es posible realizar otras operaciones sobre objetos del esquema HR, por ejemplo:

```
SELECT MAX(country_id) FROM hr.countries;
```

```
SQL Error: ORA-00942: table or view does not exist
```

```
SELECT * FROM HR.employees;
```

```
SQL Error: ORA-00942: table or view does not exist
```

```
UPDATE HR.REGIONS SET region_name = 'ASIA' WHERE region_id = 3;
```

```
SQL Error: ORA-01031: insufficient privileges
```

ROLES

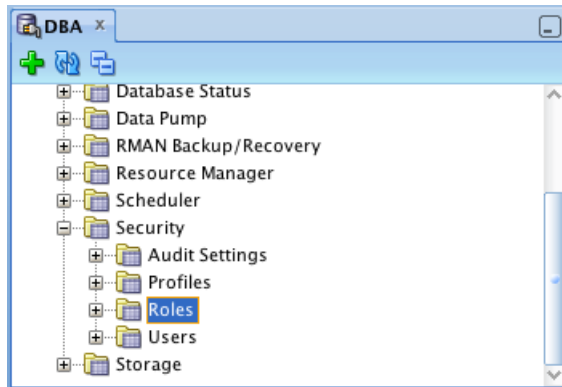
Un ROL no es más que una agrupación de privilegios bajo un nombre.

Nos permite armar un paquete de permisos que luego podrá ser asignado de diferentes usuarios. Con ello evitaremos tener que asignar permisos uno a uno.

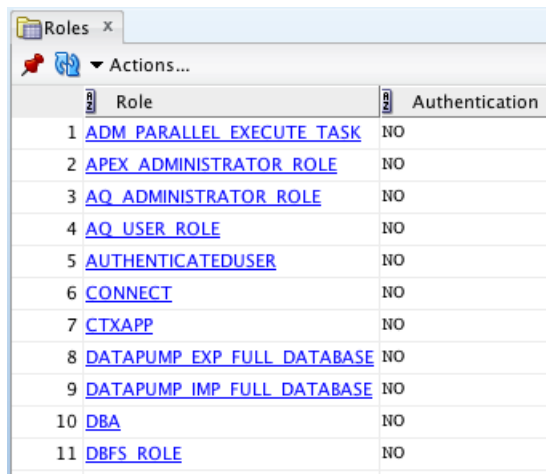
Oracle ya trae pre-configurados varios roles; los más conocidos son CONNECT y RESOURCE que ya los mencionamos antes en la creación de usuarios. Y también el rol DBA que es el que agrupa privilegios de administración de la base de datos.

Desde SQL Developer podemos revisar el contenido de esos roles, para ello:

- Accedemos al panel de administración DBA, si no aparece vamos al menú View > DBA
- Dentro del panel DBA nos conectamos como SYS
- Vamos a la rama Seguridad > Roles



- Nos aparece la lista de todos los roles precargados en Oracle



Role	Authentication
1 ADM_PARALLEL_EXECUTE_TASK	NO
2 APEX_ADMINISTRATOR_ROLE	NO
3 AQ_ADMINISTRATOR_ROLE	NO
4 AQ_USER_ROLE	NO
5 AUTHENTICATEDUSER	NO
6 CONNECT	NO
7 CTXAPP	NO
8 DATAPUMP_EXP_FULL_DATABASE	NO
9 DATAPUMP_IMP_FULL_DATABASE	NO
10 DBA	NO
11 DBFS_ROLE	NO

- Seleccionamos por ejemplo el rol RESOURCE y verificamos los permisos que éste agrupa

RESOURCE x		
General Roles Sys Privs Object Privs Consumer Group Privs User Grantees Role Grantees SQL		
Actions...		
System Privilege	Admin Option	
1 CREATE CLUSTER	NO	
2 CREATE INDEXTYPE	NO	
3 CREATE OPERATOR	NO	
4 CREATE PROCEDURE	NO	
5 CREATE SEQUENCE	NO	
6 CREATE TABLE	NO	
7 CREATE TRIGGER	NO	
8 CREATE TYPE	NO	

- Como vemos el rol RESOURCE agrupa todos los permisos para que el usuario pueda crear objetos en su esquema
- Revisemos ahora el contenido del rol DBA

DBA x		
General Roles Sys Privs Object Privs Consumer Group Privs User Grantees Role Grantees SQL		
Actions...		
System Privilege	Admin Option	
22 ALTER ANY ROLE	YES	
23 ALTER ANY RULE	YES	
24 ALTER ANY RULE SET	YES	
25 ALTER ANY SEQUENCE	YES	
26 ALTER ANY SQL PROFILE	YES	
27 ALTER ANY TABLE	YES	
28 ALTER ANY TRIGGER	YES	
29 ALTER ANY TYPE	YES	
30 ALTER DATABASE	YES	
31 ALTER PROFILE	YES	
32 ALTER RESOURCE COST	YES	
33 ALTER ROLLBACK SEGMENT	YES	
34 ALTER SESSION	YES	
35 ALTER SYSTEM	YES	
36 ALTER TABLESPACE	YES	
37 ALTER USER	YES	
38 ANALYZE ANY	YES	
39 ANALYZE ANY DICTIONARY	YES	
40 AUDIT ANY	YES	
41 AUDIT SYSTEM	YES	
42 BACKUP ANY TABLE	YES	
43 BECOME USER	YES	
44 CHANGE NOTIFICATION	YES	
45 COMMENT ANY MINING MODEL	YES	

- El rol DBA agrupa casi todos los privilegios. Por ejemplo, ALTER ANY TABLE significa que puede modificar la estructura de cualquier tabla en cualquier esquema.
- El rol DBA Incluso tiene asignados otros roles

DBA x		
General Roles Sys Privs Object Privs Consumer Group Privs User Grantees Role Grantees SQL		
Actions...		
Role	Admin Option	
1 DATAPUMP_EXP_FULL_DATABASE	NO	
2 DATAPUMP_IMP_FULL_DATABASE	NO	
3 DELETE_CATALOG_ROLE	YES	
4 EXECUTE_CATALOG_ROLE	YES	
5 EXP_FULL_DATABASE	NO	
6 GATHER_SYSTEM_STATISTICS	NO	
7 IMP_FULL_DATABASE	NO	
8 PLUSTRACE	YES	
9 SCHEDULER_ADMIN	YES	
10 SELECT_CATALOG_ROLE	YES	
11 XDBADMIN	NO	
12 XDB_SET_INVOKER	NO	

- Y por lo tanto todos los privilegios que esos roles contengan

Quiere decir entonces que cuando creamos un ROL y asignamos ese rol a un usuario, le estamos asignando al usuario todos los privilegios que ese Rol agrupa.

Un ROL oracle solamente lo puede crear un usuario con privilegios DBA (SYS, SYSTEM)

¿Cómo creamos nuestros propios roles?

En nuestro ejemplo de práctica, supongamos que con frecuencia vamos a requerir acceder al esquema HR para obtener un listado de los empleados con su cargo, salario, departamento y ciudad donde trabaja. La consulta para obtenerlo es la siguiente:

```
SELECT
    emp.EMPLOYEE_ID,
    emp.FIRST_NAME,
    emp.LAST_NAME,
    emp.EMAIL,
    emp.PHONE_NUMBER,
    car.JOB_TITLE,
    emp.SALARY,
    dep.DEPARTMENT_NAME,
    loc.CITY
FROM
    employees emp
INNER JOIN JOBS car ON emp.job_id = car.job_id
LEFT JOIN DEPARTMENTS dep ON emp.DEPARTMENT_ID = dep.DEPARTMENT_ID
LEFT JOIN LOCATIONS loc ON dep.location_id = loc.location_id;
```

14. En el esquema HR, vamos a crear una vista llamada ListaEmpleados para esa consulta. Para ello como usuario HR, ejecutamos:

```
CREATE VIEW ListaEmpleados AS
SELECT emp.EMPLOYEE_ID,
    emp.FIRST_NAME,
    emp.LAST_NAME,
    emp.EMAIL,
```

```
emp.PHONE_NUMBER,  
car.JOB_TITLE,  
emp.SALARY,  
dep.DEPARTMENT_NAME,  
loc.CITY  
FROM employees emp  
INNER JOIN JOBS car  
ON emp.job_id = car.job_id  
LEFT JOIN DEPARTMENTS dep  
ON emp.DEPARTMENT_ID = dep.DEPARTMENT_ID  
LEFT JOIN LOCATIONS loc  
ON dep.location_id = loc.location_id;
```

15. Creamos un nuevo ROL llamado RConsultaEmpleados al cual le asignaremos los siguientes permisos:

- CREATE SESSION
- CREATE TABLE
- Acceso a la vista creada anteriormente con permisos de consulta únicamente

Para ello como superusuario SYS, ejecutar:

```
CREATE ROLE RConsultaEmpleados;  
GRANT CREATE SESSION, CREATE TABLE TO RConsultaEmpleados;  
GRANT SELECT ON HR.ListaEmpleados TO RConsultaEmpleados;
```


16. Supongamos que los usuarios ana, juan y pedro necesitan acceder a consultar ese listado. Entonces crearemos esos 3 usuarios y a cada uno le asignaremos el rol creado anteriormente. Para ello como usuario SYS ejecutamos:

```
CREATE USER ana IDENTIFIED BY ana;  
CREATE USER juan IDENTIFIED BY juan;  
CREATE USER pedro IDENTIFIED BY pedro;  
GRANT RConsultaEmpleados TO ana;  
GRANT RConsultaEmpleados TO juan;  
GRANT RConsultaEmpleados TO pedro;
```

17. Nos conectamos con los usuarios creados y verificamos que efectivamente pueden consultar la vista.

```
SELECT COUNT(*) FROM HR.ListaEmpleados;  
  
COUNT(*)  
-----  
107  
  
SELECT * FROM HR.ListaEmpleados;
```

Script Output x Query R... x

 SQL | Fetched 50 rows in 0.049 seconds

	EMPLOYEE_ID	FIRST_NAME	LAST_NAME	EMAIL	PHONE_NUMBER	JOB_TITLE
1	206	William	Gietz	WGIEZT	515.123.8181	Public Accou
2	205	Shelley	Higgins	SHIGGINS	515.123.8080	Accounting M
3	200	Jennifer	Whalen	JWHALEN	515.123.4444	Administrati
4	100	Steven	King	SKING	515.123.4567	President
5	102	Lex	De Haan	LDEHAAN	515.123.4569	Administrati
6	101	Neena	Kochhar	NKOCHHAR	515.123.4568	Administrati
7	110	John	Chen	JCHEN	515.124.4269	Accountant
8	109	Daniel	Faviet	DFAVIET	515.124.4169	Accountant
9	113	Luis	Popp	LPOPP	515.124.4567	Accountant
10	111	Ismael	Sciarra	ISCIARRA	515.124.4369	Accountant
11	112	Jose Manuel	Urman	JMURMAN	515.124.4469	Accountant
12	108	Nancy	Greenberg	NGREENBE	515.124.4569	Finance Mana

Con ello cada usuario tendrá asignados los permisos contenidos en el rol, esto es: abrir una sesión, crear tablas y consultar la vista del listado en HR

CUESTIONES GENERALES

1. ¿Cuál privilegio se debe asignar a un usuario para que pueda logearse en Oracle Server?

`CREATE SESSION`

2. ¿Cuál privilegio se debe otorgar a un usuario para que pueda crear tablas?

`CREATE TABLE`

3. Usted tiene un usuario X y con él crea una tabla Z, por lo tanto, X se convierte en propietario de esa tabla Z. ¿Quién puede otorgar permisos para que otros usuarios puedan acceder a esa tabla?

Lo pueden otorgar:

- Usuarios con rol DBA (SYS, SYSTEM ..)
- Usuario X propietario de la tabla

4. Usted es un usuario con rol DBA. Y necesita crear muchos usuarios que tienen los mismos privilegios de sistema. ¿Qué puede hacer usted para facilitar el trabajo?

Primero crear un ROL y asignarle a éste todos los permisos comunes a los usuarios. Luego crear los usuarios y a cada uno asignarle el ROL creado previamente.

5. ¿Qué comando debe usar para cambiar el password de un usuario?

`ALTER USER usuario IDENTIFIED BY nuevopassword;`