

CS-3810: DB Access and Control

An important task of a database system administrator is to manage user access. This how-to illustrate how to create users with different privileges in a database using SQL Data Control Language (DCL).

Step 1: Create Database and Tables

Before proceeding on this how-to, create a database name hr and a table called Employees with the following schema (use psql tool).

```
CREATE DATABASE hr;

\c hr

CREATE TABLE Employees (
  id INT NOT NULL PRIMARY KEY,
  name VARCHAR(35) NOT NULL,
  sal INT );

INSERT INTO Employees VALUES
( 1, 'Sam Mai Tai', 35000 ),
( 2, 'Morbid Mojito', 65350 );
```

Step 2: Create Users

Create users hr and hr_admin using the following syntax.

```
CREATE USER "hr" PASSWORD '024680';
CREATE USER "hr_admin" PASSWORD '135791';
```

Step 3: Verify Users

All users in Postgres are saved internally. You can list them using:

```
\du
```

Verify that users hr and hr_admin are listed.

Role name	List of roles Attributes	Member of
hr		{ }
hr_admin		{ }
postgres	Superuser, Create role, Create DB, Replication, Bypass RLS	{ }
tmota	Superuser, Create role, Create DB	{ }

Step 4: Grant Access to the Users

We want to restrict access of user hr to SELECT operations on table Employees. On the other hand, user hr_admin should be granted full access to the table. Below are the commands you use to grant specific access to users on a table.

```
GRANT SELECT ON TABLE Employees TO "hr";  
GRANT ALL ON TABLE Employees TO "hr_admin";
```

Step 5: Test User Access

Now logoff from psql and login again as user hr. Try to issue a query and an INSERT. The later operation should fail because user hr access was restricted to SELECT operations only.

On the terminal:

```
psql -d hr -U hr -W
```

On psql tool, let's give Thyago a 200K salary.

```
INSERT INTO Employees VALUES (3, 'Thyago', 200000);
```

It should NOT work!

```
ERROR:  permission denied for table employees
```

Now try select on table Employees. It should work!

Logoff from postgres and repeat the insert statement, but now logged in as hr_admin. It should work!

There is much more about user access control. For example, you can grant access to a user on different object types, not only on a table but to a whole database, for example. There are also many other grant privilege levels other than the ones described here.