Data Control Language (DCL)
Seguretat en una Base de Dades

Institut Rafael Campalans
Plaça del Remei, 1
17160 Anglès

Cicle: DAM
Curs: 2022/2023
Mòdul: 02 Bases de Dades

Objectius

- Conèixer els mecanismes per establir seguretat dintre de una base de dades
  - Seguretat de sistema
  - Seguretat de les dades
- Creació de rols.
- Atorgar i denegar privilegis. GRANT/REVOKE

Seguretat a la base de dades

La seguretat en la base de dades es classifica en dues categories:

- **Seguretat del sistema**: Controla l'accés i ús de la base de dades a nivell de sistema (accessos, crear, modificar objectes)

- **Seguretat de les dades**: Controla l'accés i ús de la base de dades a nivell d'objectes (permisos de select, update, … sobre taules, vistes, etc.)

Creació d'usuaris - ROLS

- A diferencia d'altres SGBD Postgresql no treballa amb el concepte d'usuari sinó amb el concepte de rol.
- Alguns rols permeten realitzar un login a la base de dades, serien els equivalents al usuaris d'altres SGBD.
- Els rols que poden contenir altres rols s'anomenen rols de grup, serien equivalents als rols d'altres SGBD.

La sentència CREATE ROLE (CREATE USER)

```
CREATE ROLE role_name;
```

```
CREATE ROLE role_name
LOGIN
PASSWORD 'role_passwd';
```

```
SELECT rolname FROM pg_roles;
```

```
 rolname
------------------------------
 pg_monitor
 pg_read_all_settings
...
 postgres
 bob
```

La sentència CREATE ROLE - Exemples

```
CREATE ROLE john
SUPERUSER
LOGIN
PASSWORD 'securePass1';
```

```
CREATE ROLE dba
CREATEDB
LOGIN
PASSWORD 'Abcd1234';
```

ALTER ROLE i DROP ROLE

```
ALTER ROLE role_name [WITH] option;
```

```
ALTER ROLE calf SUPERUSER;

ALTER ROLE calf PASSWORD '1234';
```

```
DROP ROLE [IF EXISTS] target_role;
```

```
DROP ROLE calf;
```

La sentència GRANT

- Privilegis de sistema:

```
GRANT { { CREATE | CONNECT | TEMPORARY | TEMP}
| ALL [ PRIVILEGES ] }
ON DATABASE database_name
TO { [ GROUP ] role_name | PUBLIC }
[ WITH GRANT OPTION ]

GRANT { { CREATE | USAGE} | ALL [ PRIVILEGES ] }
ON SCHEMA schema_name
TO { [ GROUP ] role_name | PUBLIC }
[ WITH GRANT OPTION ]
```

La sentència GRANT

```
GRANT USAGE ON SCHEMA hr
TO calf;

GRANT CONNECT ON DATABASE hr
TO hruser;

GRANT CREATE, USAGE ON SCHEMA hr
TO alice;

GRANT ALL PRIVILEGES
ON DATABASE hr
TO dba
WITH GRANT OPTIONS;
```

La sentència GRANT

- Privilegis sobre dades:

```
GRANT { { SELECT | INSERT | UPDATE | DELETE | REFERENCES
| TRIGGER | TRUNCATE [,…]| ALL [ PRIVILEGES ] }
ON {[TABLE] table_name |
ALL TABLES IN SCHEMA schema_name }
TO { [ GROUP ] role_name | PUBLIC }[ WITH GRANT OPTION ]
```

```
GRANT { { SELECT | INSERT | UPDATE | REFERENCES }
(column, [,…])
 | ALL [ PRIVILEGES ] (column, [,…]) }
ON {[TABLE] table_name |
TO { [ GROUP ] role_name | PUBLIC }[ WITH GRANT OPTION ]
```

La sentència GRANT

- Assignar privilegis de:

```
GRANT SELECT
ON candidates
TO joe;

GRANT INSERT, UPDATE, DELETE
ON candidates
TO joe;

GRANT ALL
ON ALL TABLES
IN SCHEMA "public"
TO joe;
```

```
GRANT SELECT ON employees
TO PUBLIC

GRANT SELECT(first_name),
UPDATE(hire_date)
ON employees
TO alice;

GRANT ALL PRIVILEGES
ON departments
TO manuel
```

La sentència REVOKE

- Privilegis de sistema:

```
REVOKE [GRANT OPTION FOR]
{ { CREATE | CONNECT | TEMPORARY | TEMP}
| ALL [ PRIVILEGES ] }
ON DATABASE database_name
FROM { [ GROUP ] role_name | PUBLIC }
[ CASCADE | RESTRICT ]

REVOKE [GRANT OPTION FOR]
{ { CREATE | USAGE} | ALL [ PRIVILEGES ] }
ON SCHEMA schema_name
FROM { [ GROUP ] role_name | PUBLIC }
[ CASCADE | RESTRICT ]
```

La sentència REVOKE

```
REVOKE [GRANT OPTION FOR]
{ { SELECT | INSERT | UPDATE | DELETE | REFERENCES
| TRIGGER | TRUNCATE [,…]| ALL [ PRIVILEGES ] }
ON {[TABLE] table_name |
ALL TABLES IN SCHEMA schema_name }
FROM { [ GROUP ] role_name | PUBLIC }
[ CASCADE | RESTRICT ]


REVOKE [GRANT OPTION FOR]
{ { SELECT | INSERT | UPDATE | REFERENCES }
(column, [,…])
 | ALL [ PRIVILEGES ] (column, [,…]) }
ON {[TABLE] table_name |
FROM { [ GROUP ] role_name | PUBLIC }
[ CASCADE | RESTRICT ]
```

La sentència REVOKE

- Privilegis sobre dades:

```
REVOKE ALL PRIVILEGES
ON employees FROM manuel;

REVOKE INSERT
ON films FROM PUBLIC;

REVOKE GRANT OPTION FOR CONNECT  ON
DATABASE hr
FROM hruser CASCADE;
```

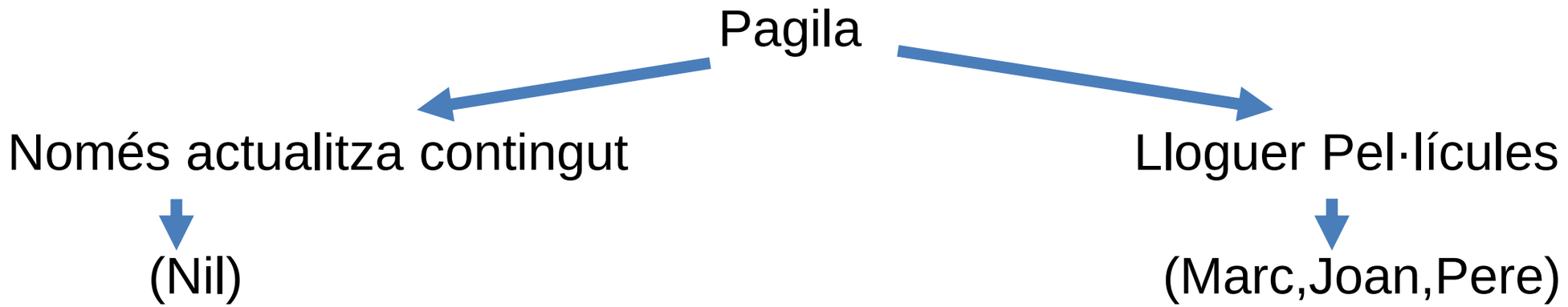
Rols de grup

- Es habitual utilitzar rols per agrupar privilegis de diferents usuaris.
- Normalment crearem un rol que representarà a un grup al que afegirem altres membres (roles amb login (usuaris) i/o rols de grup)
- Per convenció un rol de grup serà aquell que no tindrà permís de Login.

```
CREATE ROLE role_group_name;
```

```
GRANT role_group_name TO user_role;
```

Exemple




```
CREATE ROLE nomes_contingut;
CREATE ROLE nil LOGIN password ‘123’;

GRANT SELECT ON film
TO nomes_contingut;

GRANT nomes_contingut to nil;
```

```
CREATE ROLE lloguer;
CREATE ROLE Marc LOGIN password ‘123’;
CREATE ROLE Joan LOGIN password ‘123’;
CREATE ROLE Pere LOGIN password ‘123’;

GRANT ALL IN ALL TABLES TO lloguer;

GRANT lloguer to Marc,joan,Pere;
```

Rols de grup - Exemples

- Un usuari pot tenir permisos sobre un objecte per si mateix o bé per estar en un rol de grup.

```
CREATE ROLE sales;

GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public
TO sales;

GRANT SELECT ON rental TO alice;

GRANT sales TO alice;
```

Rols de grup - Exemples

```
Postgresql$ psql -d pagila -U alice

Pagila=> SELECT * FROM film;
…
Pagila=> SELECT * FROM actor;
…
Pagila=>\c pagila postgres;
Pagila=>REVOKE sales FROM alice;

Pagila=>\c pagila alice;
Pagila=>SELECT * FROM actor;
ERROR: Permission denied for relation actor
```

Resum

Sentència	Descripció
CREATE/ALTER/DROP DATABASE	Creació, modificació i eliminació de bases de dades.
CREATE/ALTER/DROP ROLE	Creació, modificació i eliminació de rols.
GRANT	Atorgar privilegis (permisos) sobre objectes de la base de dades.
REVOKE	Revocar privilegis (permisos) sobre objectes de la base de dades.

Activitat A01

Gestió d'usuaris

- Connectat al Moodle i descarrega't la pràctica "A01 Gestió d'usuaris".
- Temps 90m

WEBGRAFIA

- SQL Tutorial, W3schools, Setembre 2022, https://www.w3schools.com/sqL/default.asp
- PostgreSQL Tutorial from scratch, Setembre 2022, https://www.postgresqltutorial.com/
- Exercicis Online de SQL, W3schools, Setembre 2022, https://www.w3schools.com/SQl/sql_exercises.asp
- PostgreSQL Exercices, Practice,Solution, W3resource,Setembre 2022, https://www.w3resource.com/postgresql-exercises/
- PostgreSQL Documentation, PostgreSQL, Setembre 2022, https://www.postgresql.org/docs/