



Transações + Roles e permissões



Professor

Fernando Martins Medeiros

Transações

Quando tratamos de concorrência em SGBD, a primeira ideia que deve vir a mente são as “**Transações**”, pois estas podem garantir a **execução** de **múltiplas threads** em um **mesmo instante de tempo**.

Transações

```
1  BEGIN - -iniciar
2  - -   comandos
3  COMMIT - -comitar/confirmar
4  ROLLBACK - -parar/cancelar
5  END - -memsa função do COMMIT
```

Transações

```
BEGIN;  
UPDATE aluno SET nome = 'ALUNO 1' WHERE id = 2;  
INSERT INTO aluno (login, nome) VALUES ('ALUNO 2', 'Nome completo do aluno');  
DELETE FROM aluno WHERE id = 3;  
COMMIT;  
--ROLLBACK;
```

Transações

```
-- TRANSACAO 1
BEGIN;
UPDATE aluno SET nome = 'ALUNO 1' WHERE id = 2;
INSERT INTO aluno (login, nome) VALUES ('ALUNO 2', 'Nome completo do aluno');
COMMIT;

-- TRANSACAO 2
BEGIN;
DELETE FROM aluno WHERE id = 3;
DELETE FROM aluno WHERE id = 4;
COMMIT;
```

Roles e permissões

O comando **CREATE ROLE** adiciona um novo papel (role) ao agrupamento de bancos de dados do PostgreSQL. O papel é uma entidade que pode possuir objetos do banco de dados e possuir privilégios do banco de dados. Ele pode ser considerado como sendo um "usuário", um "grupo", ou ambos, dependendo de como é utilizado

```
CREATE ROLE name [ [ WITH ] option [ ... ] ]
```

where *option* can be:

```
    SUPERUSER | NOSUPERUSER  
| CREATEDB | NOCREATEDB  
| CREATEROLE | NOCREATEROLE  
| CREATEUSER | NOCREATEUSER  
| INHERIT | NOINHERIT  
| LOGIN | NOLOGIN  
| CONNECTION LIMIT connlimit  
| [ ENCRYPTED | UNENCRYPTED ] PASSWORD 'password'  
| VALID UNTIL 'timestamp'  
| IN ROLE rolename [, ...]  
| IN GROUP rolename [, ...]  
| ROLE rolename [, ...]  
| ADMIN rolename [, ...]  
| USER rolename [, ...]  
| SYSID uid
```

Roles e permissões

Opção	Descrição
SUPERUSER NOSUPERUSER	Estas cláusulas determinam se o novo papel é um "super-usuário", o qual pode passar por cima de todas as restrições de acesso dos bancos de dados. Se nenhuma destas duas cláusulas for especificada, o padrão é NOSUPERUSER.
CREATEDB NOCREATEDB	Estas cláusulas definem a permissão para o papel criar bancos de dados. Se nenhuma destas duas cláusulas for especificada, o padrão é NOCREATEDB.
CREATEROLE NOCREATEROLE	Estas cláusulas determinam se o papel terá permissão para criar novos papéis (ou seja, executar o comando CREATE ROLE).
CREATEUSER NOCREATEUSER	Estas cláusulas são formas obsoletas, mas ainda aceitas, das cláusulas SUPERUSER e NOSUPERUSER.
INHERIT NOINHERIT	Estas cláusulas determinam se o papel "herda" os privilégios dos papéis dos quais é membro. Um papel com o atributo INHERIT pode utilizar, automaticamente, todos os privilégios de banco de dados que foram concedidos a todos os papéis dos quais é um membro direto ou indireto.
LOGIN NOLOGIN	Estas cláusulas determinam se o papel pode estabelecer uma conexão (log in), ou seja, se o papel pode ser fornecido como nome de autorização inicial da sessão durante a conexão do cliente. Um papel com o atributo LOGIN pode ser considerado como sendo um usuário. Se nenhuma destas duas cláusulas for especificada, o padrão é NOLOGIN, exceto quando CREATE ROLE for chamada através de sua forma alternativa CREATE USER.
CONNECTION LIMIT limite_de_conexões	Se o papel puder estabelecer uma conexão, esta cláusula especifica quantas conexões simultâneas este papel pode estabelecer. -1 (o padrão) significa sem limite.
PASSWORD senha	Define a senha do papel (A senha só é útil para os papéis que possuem o atributo LOGIN, mesmo assim pode ser definida uma senha para os papéis sem este atributo).
ENCRYPTED UNENCRYPTED	Estas cláusulas controlam se a senha será armazenada criptografada, ou não, nos catálogos do sistema;
VALID UNTIL 'carimbo_do_tempo'	A cláusula VALID UNTIL define uma data e hora após a qual o papel não é mais válido. Se esta cláusula for omitida, a senha será válida para sempre.
IN ROLE nome_do_papel	A cláusula IN ROLE relaciona um ou mais papéis existentes, aos quais o novo papel será adicionado imediatamente como sendo um novo membro.
IN GROUP nome_do_papel	A cláusula IN GROUP é uma forma obsoleta de IN ROLE.
ROLE nome_do_papel	A cláusula ROLE relaciona um ou mais papéis existentes a serem automaticamente adicionados como membros do novo papel (Isto tem como efeito tornar o novo papel um "grupo").
ADMIN nome_do_papel	A cláusula ADMIN é como a cláusula ROLE, mas os papéis especificados são adicionados ao novo papel WITH ADMIN OPTION, dando aos mesmos o direito de permitir que outros papéis se tornem membros deste grupo.
USER nome_do_papel	A cláusula USER é uma forma obsoleta da cláusula ROLE.
SYSID id_usuário	A cláusula SYSID é ignorada, mas é aceita para manter a compatibilidade com as versões anteriores.

Roles – Criando uma nova role

```
CREATE ROLE fernando_martins LOGIN PASSWORD '123456';
```


GRANT – Define privilégios de acesso

O comando **GRANT** possui duas funcionalidades básicas: conceder **privilégios** para um objeto do banco de dados (tabela, visão, seqüência, banco de dados, função, linguagem procedural, esquema e espaço de tabelas), e conceder o privilégio de ser **membro** de um **papel**;

```
GRANT { { SELECT | INSERT | UPDATE | DELETE | REFERENCES | TRIGGER }
        [,...] | ALL [ PRIVILEGES ] }
ON [ TABLE ] nome_da_tabela [, ...]
TO { nome_do_usuario | GROUP nome_do_grupo | PUBLIC } [, ...] [ WITH GRANT OPTION ]

GRANT { { USAGE | SELECT | UPDATE }
        [,...] | ALL [ PRIVILEGES ] }
ON SEQUENCE nome_da_seqüencia [, ...]
TO { nome_do_usuario | GROUP nome_do_grupo | PUBLIC } [, ...] [ WITH GRANT OPTION ]

GRANT { { CREATE | CONNECT | TEMPORARY | TEMP } [,...] | ALL [ PRIVILEGES ] }
ON DATABASE nome_do_banco_de_dados [, ...]
TO { nome_do_usuario | GROUP nome_do_grupo | PUBLIC } [, ...] [ WITH GRANT OPTION ]

GRANT { EXECUTE | ALL [ PRIVILEGES ] }
ON FUNCTION nome_da_função ( [ [ modo_do_argumento ] [ nome_do_argumento ] tipo_do_argumento [, ...] ] ) [, ...]
TO { nome_do_usuario | GROUP nome_do_grupo | PUBLIC } [, ...] [ WITH GRANT OPTION ]

GRANT { USAGE | ALL [ PRIVILEGES ] }
ON LANGUAGE nome_da_linguagem [, ...]
TO { nome_do_usuario | GROUP nome_do_grupo | PUBLIC } [, ...] [ WITH GRANT OPTION ]

GRANT { { CREATE | USAGE } [,...] | ALL [ PRIVILEGES ] }
ON SCHEMA nome_do_esquema [, ...]
TO { nome_do_usuario | GROUP nome_do_grupo | PUBLIC } [, ...] [ WITH GRANT OPTION ]

GRANT { CREATE | ALL [ PRIVILEGES ] }
ON TABLESPACE nome_do_espaco_de_tabelas [, ...]
TO { nome_do_usuario | GROUP nome_do_grupo | PUBLIC } [, ...] [ WITH GRANT OPTION ]

GRANT role [, ...] TO nome_do_usuario [, ...] [ WITH ADMIN OPTION ]
```

GRANT – Define privilégios de acesso

```
GRANT SELECT, UPDATE, INSERT, TRIGGER ON auditoria TO fernando_martins;
```

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO fernando_martins;
```

REVOKE – Revoga privilégios de acesso

O comando **REVOKE** revoga, de um ou mais papéis, privilégios concedidos anteriormente. A palavra chave PUBLIC se refere ao grupo contendo todos os usuários, definido implicitamente.

```
REVOKE [ GRANT OPTION FOR ]
{ { SELECT | INSERT | UPDATE | DELETE | REFERENCES | TRIGGER }
[,...] | ALL [ PRIVILEGES ] }
ON [ TABLE ] nome_da_tabela [, ...]
FROM { nome_do_usuario | GROUP nome_do_grupo | PUBLIC } [, ...]
[ CASCADE | RESTRICT ]

REVOKE [ GRANT OPTION FOR ]
{ { USAGE | SELECT | UPDATE }
[,...] | ALL [ PRIVILEGES ] }
ON SEQUENCE nome_da_sequência [, ...]
FROM { nome_do_usuario | GROUP nome_do_grupo | PUBLIC } [, ...]
[ CASCADE | RESTRICT ]

REVOKE [ GRANT OPTION FOR ]
{ { CREATE | CONNECT | TEMPORARY | TEMP } [,...] | ALL [ PRIVILEGES ] }
ON DATABASE nome_do_banco_de_dados [, ...]
FROM { nome_do_usuario | GROUP nome_do_grupo | PUBLIC } [, ...]
[ CASCADE | RESTRICT ]

REVOKE [ GRANT OPTION FOR ]
{ EXECUTE | ALL [ PRIVILEGES ] }
ON FUNCTION nome_da_função ( [ [ modo_do_argumento ] [ nome_do_argumento ] tipo_do_argumento [, ...] ] ) [, ...]
FROM { nome_do_usuario | GROUP nome_do_grupo | PUBLIC } [, ...]
[ CASCADE | RESTRICT ]

REVOKE [ GRANT OPTION FOR ]
{ USAGE | ALL [ PRIVILEGES ] }
ON LANGUAGE nome_da_linguagem [, ...]
FROM { nome_do_usuario | GROUP nome_do_grupo | PUBLIC } [, ...]
[ CASCADE | RESTRICT ]

REVOKE [ GRANT OPTION FOR ]
{ { CREATE | USAGE } [,...] | ALL [ PRIVILEGES ] }
ON SCHEMA nome_do_esquema [, ...]
FROM { nome_do_usuario | GROUP nome_do_grupo | PUBLIC } [, ...]
[ CASCADE | RESTRICT ]

REVOKE [ GRANT OPTION FOR ]
{ CREATE | ALL [ PRIVILEGES ] }
ON TABLESPACE nome_do_espaco_de_tabelas [, ...]
FROM { nome_do_usuario | GROUP nome_do_grupo | PUBLIC } [, ...]
[ CASCADE | RESTRICT ]

REVOKE [ ADMIN OPTION FOR ]
role [, ...] FROM nome_do_usuario [, ...]
[ CASCADE | RESTRICT ]
```

Montando o ambiente...

<https://trier.link/GzdRc1ioJ>