Controle de acesso e privilégios

TIAGO G MORAES

Roteiro

- Introdução
- Controle de Usuários
- Controle de Papéis
- Controle de Privilégios

Introdução

- Motivação:
  - Muitas pessoas se conectaram a um determinado banco de dados
  - Essas pessoas devem ter permissões de acesso e manipulação específicas para:
    - Banco de dados
    - Tabelas
    - Views
    - Stored Procedures
- Em SQl o pacote que manipula as definições de usuário e permissões é a DCL
  - DCL : Data Control Language

Controle de Usuários

- Criação de um usuário
  - CREATE USER

```
CREATE USER <nome_user>
[WITH <option1> [<option2> ...]]
```

- Options:
  - CREATEDB ou **NOCREATEDB** → pode ou não criar BDs
  - SUPERUSER ou **NOSUPERUSER** → super usuário ou não
  - CREATEROLE ou **NOCREATEROLE** → se pode criar novos papéis
  - IN ROLE <nome papel> → já adiciona o usuário em um ou mais papéis
  - ENCRYP TED PASSWORD '<senha>' → atribui senha ao novo user

Controle de Usuários

- Criação de um usuário
  - CREATE USER

```
CREATE USER <nome_user>
[WITH <option1> [<option2> ...]]
```

- Options:
  - CREATEDB ou **NOCREATEDB** → pode ou não criar BDs
  - SUPERUSER ou **NOSUPERUSER** → super usuário ou não
  - CREATEROLE ou **NOCREATEROLE** → se pode criar novos papéis
  - IN ROLE <nome papel> → já adiciona o usuário em um ou mais papéis
  - ENCRYP TED PASSWORD '<senha>' → atribui senha ao novo user

→default

→[] = opcionalidade →<> = preencher com algum valor →{} = escolha um dos itens

Controle de Usuários

- Criação de um usuário
  - CREATE USER
- No postgres:
  - user padrão: **postgres**
  - postgres também é o usuário **root** ou **superuser**
  - No psql: "\du" → ver os usuários
  - Ou:

```
SELECT * FROM pg_user
        ou
SELECT * FROM pg_roles
```

Controle de Usuários

- Excluir um usuário
  - DROP USER

```
DROP USER <nome_user>
```

- Alterar um usuário
  - ALTER USER

```
ALTER USER <nome_user>
WITH <option1> [<option2> ...]
```


Controle de Papéis

- Papéis são uma forma de agrupar usuários
- Por exemplo: ao invés de se criar um usuário aluno e todos alunos se conectarem por esse usuário,
  - cria-se um usuário para cada aluno;
  - e um papel aluno;
  - vincula-se o papel a cada usuário criado.
- Os papéis podem estar vinculados a outros papéis
  - Criando uma hierarquia de papéis
  - Desta forma um usuário terá os privilégios (permissões) atribuídas:
    - Diretamente ao seu usuário
    - Aos seus papéis
    - Aos papéis atribuídos aos seus papéis e assim sucessivamente

Controle de Papéis

- Criar um papel
  - CREATE ROLE : equivalente a CREATE USER

```
CREATE ROLE <nome_user>
[WITH <option1> [<option2> ...]]
```

- Excluir um papel
  - DROP ROLE: equivalente a DROP USER

```
DROP ROLE <nome_user>
```

- Alterar um papel
  - ALTER ROLE: equivalente a ALTER USER

```
ALTER ROLE <nome_user>
WITH <option1> [<option2> ...]
```


Controle de Papéis

- Atribuindo papéis
  - GRANT

```
GRANT <nome_role>
TO <user/role>, <user2/role> ...
```

- Retirando um papel
  - REVOKE

```
REVOKE <nome_role> FROM
<user/role>, <user2/role> ...
```


Controle de Privilégios

- Alguns Tipos de privilégio:
  - CONNECT (em BD)
  - SELECT (em tabela)
  - UPDATE (em tabela)
  - INSERT (em tabela)
  - DELETE (em tabela)
  - EXECUTE (em stored procedure ou function)

Pode especificar as colunas:
Ex: ...SELECT(nome) ON pessoa...

- Sintaxe para conceder privilégios

```
GRANT <nome_privilégio>
ON {<nome table>|DATABASE <nome bd>|FUNCTION <nome_funcao>}
TO <nome_role/nome_user>,...
```


Controle de Privilégios

- Sintaxe para retirar privilégios

```
REVOKE <nome_privilégio>
ON {<nome table>|DATABASE <nome bd>|FUNCTION <nome_funcao>}
FROM <nome_role/nome_user>,...
```

- Exemplos:

1. REVOKE update(nome) ON departamento FROM estagiario, analista
2. GRANT all privileges ON funcionario, projeto TO estagiario
3. GRANT connect ON DATABASE base1 TO estagiario
4. REVOKE execute ON FUNCTION func_1() FROM estagiario

Controle de Privilégios

- No postgres:
  - "\dp" ou "\z" → visualiza privilégios de tabelas, sequencias e *views*
  - Mostra quando já foi definido algum privilégio diferente dos default na tabela
    - Legenda: <user>=permissões/dono
    - Onde permissões pode ser:
      - a = inserir
      - w = update
      - r = select
      - d = deletar
      - D = truncate
      - x = references
      - t = trigger
  - "\l" → visualiza privilégios de banco de dados
  - Mostra quando já foi definido algum privilégio diferente dos default no bd
    - Legenda: <user>=permissões/dono
    - Onde permissões pode ser:
      - X = execute
      - U = usage
      - c = connect
      - C = Create
      - T = temporary

Controle de Privilégios

- Outros tópicos:
  - Controle de acesso para linhas ?
  - Passar minhas permissões adiante ?
  - Permissão de criar novas ROLES ?
  - Papel geral no postgres: public