Instituto Federal Sul-Riograndense

Autorizações de Acesso

Prof. Alexandre Tagliari Lazzaretti
lazzaretti10@gmail.com

Autorização de Acesso

- Objetivo
  - proteção contra acessos mal intencionados
- Subsistema de Autorização de Acesso (SAA)
  - controla quais dados um usuário/grupo de usuários pode ter acesso
  - controle quais operações um usuário/grupo de usuários pode realizar sobre estes dados
- Funções do subsistema de autorização
  - especificação de autorizações
  - verificação de autorizações

Funções do Subsistema de AA

- Cadastro de usuários/grupos
  - *login* + *password*
- Especificação de autorizações
  - envolve três dimensões
    - agente (usuário ou grupo)
    - grânulo (BD, tabela, atributos, atributo, tuplas, ...)
    - operação (*select*, *update*, *create*, ...)
  - DBA
    - superusuário (pode tudo!)
      - alguns privilégios são exclusivos dele
        - » *recovery* BD, configuração parâmetros do SGBD, ...
    - concede/retira (revoga) privilégios de acesso
  - outros agentes
    - todos os privilégios de acesso aos grânulos (BDs e tabelas) que criou
    - concede/revoga privilégios para estes grânulos a outros agentes

Classificação de AA

1. Baseadas no grânulo + operação
   - é ou não válido para todos os usuários
     - permissões públicas ou secretas
2. Baseadas nas três dimensões
   - grânulo + operação + agente
   - utiliza matrizes de autorização de acesso
3. Baseadas em restrições
   - utiliza visões

Matriz de AA

	G_1	G_2	G_3	. . .	G_n
A_1	*select*	*select, insert*			*create*
A_2			*select, update*		
A_3	*select, delete, exec*				*select, update, grant*
...					
A_m		*create*	*select, insert*		

A (Agente): Usuário ou grupo

G (Grânulo): BD, tabela, ...

Outras Considerações sobre AA

- Premissa básica
  - "quem não consulta não pode atualizar"
- Ações na ocorrência de violações
  - podem ser configuradas pelo DBA
    - mensagens de advertência
    - registro de tentativas
    - bloqueio de acesso
- Administrar corretamente permissões sobre tabelas e visões
  - exemplo
    - não faz sentido uma mesma permissão sobre uma tabela base e uma visão derivada dela

Comandos em SQL

- Grant
  - O comando GRANT concede privilégios de acesso aos objetos criados no banco de dados
- Revoke
  - O comando REVOKE revoga os privilégios de acesso aos objetos do banco de dados.

Granularidade dos objetos

- SELECT
- INSERT
- UPDATE
- DELETE
- REFERENCES
- TRIGGER
- CONNECT
- TEMPORARY
- EXECUTE
- USAGE

- SELECT

Permite consultar (SELECT) qualquer coluna da tabela, visão ou seqüência especificada. Também permite utilizar o comando COPY TO. Para as seqüências, este privilégio também permite o uso da função currval.

INSERT

Permite inserir (INSERT) novas linhas na tabela especificada. Também permite utilizar o comando COPY FROM.

UPDATE

Permite modificar (UPDATE) os dados de qualquer coluna da tabela especificada. O comando SELECT ... FOR UPDATE também requer este privilégio (além do privilégio SELECT). Para as seqüências, este privilégio permite o uso das funções nextval e setval.

DELETE

Permite excluir (DELETE) linhas da tabela especificada.

RULE

Permite criar regras para a tabela ou para a visão (Consulte o comando CREATE RULE).

- REFERENCES

Para criar uma restrição de chave estrangeira é necessário possuir este privilégio, tanto na tabela que faz referência quanto na tabela que é referenciada.

TRIGGER

Permite criar gatilhos na tabela especificada (Consulte o comando CREATE TRIGGER).

CREATE
Para bancos de dados, permite a criação de novos esquemas no banco de dados.

Para esquemas, permite a criação de novos objetos no esquema. Para mudar o nome de um objeto existente é necessário ser o dono do objeto e possuir este privilégio no esquema que o contém.

Para espaços de tabelas, permite a criação de tabelas e índices no espaço de tabelas, e permite a criação de bancos de dados possuindo este espaço de tabelas como seu espaço de tabelas padrão (Deve ser observado que revogar este privilégio não altera a colocação dos objetos existentes).

TEMPORARY
TEMP
Permite a criação de tabelas temporárias ao usar o banco de dados.

EXECUTE
Permite utilizar a função especificada e qualquer operador implementado utilizando a função. Este é o único tipo de privilégio aplicável às funções (Esta sintaxe funciona para as funções de agregação também).

USAGE
Para as linguagens procedurais, permite o uso da linguagem especificada para criar funções nesta linguagem. Este é o único tipo de privilégio aplicável às linguagens procedurais.

Para os esquemas, permite acessar os objetos contidos no esquema especificado (assumindo que os privilégios requeridos para os próprios objetos estejam atendidos). Essencialmente, concede a quem recebe o direito de "procurar" por objetos dentro do esquema.

ALL PRIVILEGES
Concede todos os privilégios disponíveis de uma só vez. A palavra chave PRIVILEGES é opcional no PostgreSQL, embora seja requerida pelo SQL estrito.

GRANT

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

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

GRANT { EXECUTE | ALL [ PRIVILEGES ] }
    ON FUNCTION nome_da_função ([tipo, ...]) [, ...]
    TO { nome_do_usuário | GROUP nome_do_grupo | PUBLIC } [, ...] [ WITH GRANT OPTION ]

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

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

GRANT { CREATE | ALL [ PRIVILEGES ] }
    ON TABLESPACE nome_do_espaço_de_tabelas [, ...]
    TO { nome_do_usuário | GROUP nome_do_grupo | PUBLIC } [, ...] [ WITH GRANT OPTION ]
```

Exemplos

- `GRANT INSERT ON filmes TO PUBLIC;`
- `GRANT ALL PRIVILEGES ON vis_tipos TO manuel;`
- `GRANT SELECT ON minha_tabela TO PUBLIC;`
- `GRANT SELECT, UPDATE, INSERT ON minha_tabela TO GROUP todos;`

- Para consultar as tabelas do banco:

```
Select * from pg_tables
```

REVOKE

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

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

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

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

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

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

Exemplos

- `REVOKE INSERT ON filmes FROM PUBLIC;`
- `REVOKE ALL PRIVILEGES ON vis_tipos FROM manuel;`