Prof. Taciano Balardin

www.taciano.pro.br

taciano@ulbra.edu.br

2015-2

Banco de Dados II

E-MAIL DE CONTATO:
taciano@ulbra.edu.br

SITE DA DISCIPLINA:
http://www.taciano.pro.br/

Controle de Usuários e Políticas de Acesso

BANCO DE DADOS II
AULA 16

Prof. Taciano Balardin

Controle de Usuários e Políticas de Acesso

- Todo agrupamento de **bancos de dados possui um conjunto de usuários**.
- Estes usuários são **distintos dos usuários gerenciados pelo sistema operacional** onde o servidor executa.
- Os usuários possuem objetos de banco de dados (por exemplo, tabelas), e podem **conceder privilégios nestes objetos** para outros usuários controlando, assim, **quem pode acessar qual objeto**.
- Podemos ter **diferentes usuários** do banco de dados e **cada um pode ter diferentes privilégios**.

Criando um Usuário

Criando um usuário **taciano**, que se conectara a partir de **localhost**, com a senha **123456**

```
mysql> CREATE USER 'taciano'@'localhost' IDENTIFIED BY '123456';
```

localhost → indica o endereço IP a partir do qual aquele usuário tem permissão para acessar o banco de dados.

Se quisermos atribuir acesso a partir de qualquer endereço devemos utilizar o **'%'**.

Também é possível definir uma faixa de IP utilizando o **'192.%'**.

Manipulando um Usuário

Definindo uma nova senha para o usuário **taciano@localhost**:

```
mysql> SET PASSWORD FOR 'taciano'@'localhost' = PASSWORD('12345');
```

Visualizando os privilégios do usuário **taciano@localhost**:

```
mysql> SHOW GRANTS FOR 'taciano'@'localhost'
```

Excluindo o usuário **taciano@localhost**:

```
mysql> DROP USER 'taciano'@'localhost';
```

Privilégios

- O sistema de privilégios garante que **qualquer usuário possa fazer exatamente as operações que lhe é permitido**.
  - Quando conectado a um servidor, a **identidade** de um usuário é determinada pela **máquina de onde ele se conectou** e pelo **nome de usuário** que especificou.
  - O sistema concede **privilégios de acordo com a identidade** e com **o que o usuário deseja fazer**.

Privilégios

Privilégio	Descrição
CREATE	Permite executar CREATE
DROP	Permite executar DROP
ALTER	Permite executar ALTER TABLE
DELETE	Permite executar DELETE
GRANT OPTION	Permite repassar privilégios
LOCK TABLES	Permite executar LOCK TABLES em tabelas com privilégio SELECT
INDEX	Permite executar CREATE INDEX e DROP INDEX
INSERT	Permite executar INSERT
SELECT	Permite executar SELECT
UPDATE	Permite executar UPDATE
TRIGGER	Criar, excluir ou executar um TRIGGER

Privilégios

Privilégio	Descrição
CREATE VIEW	Criar VIEW
ALTER ROUTINE	Alterar ou excluir uma rotina (stored procedure ou function)
CREATE ROUTINE	Criar uma rotina (stored procedure ou function)
EXECUTE	Executar uma rotina (stored procedure ou function)
FILE	Ler ou gerar arquivos com LOAD DATA INFILE e SELECT INTO OUTFILE
CREATE USER	Criar, alterar, excluir ou renomear um usuário
PROCESS	Permite visualizar informações com SHOW FULL PROCESSLIST
SHOW DATABASES	Permite visualizar tabelas com SHOW DATABASES
SHUTDOWN	Permite utilizar o comando SHUTDOWN
USAGE	Sinônimo para “sem previlégios”
ALL	

Privilégios

- Após informar os privilégios do usuário, indica-se o nível ao qual o privilégio se aplica, sendo possível conceder e revogar direitos aos usuários em quatro níveis:
  - **Nível global** – Privilégios globais aplicam para todos os bancos de dados em um determinado servidor. **GRANT ALL ON *.*** (**conceder** o direto) e **REVOKE ALL ON *.*** (**revogar** o direito)
  - **Nível dos bancos de dados** – Privilégios de bancos de dados aplicam-se a todas as tabelas em um determinado banco de dados. **GRANT ALL ON db.*** e **REVOKE ALL ON db.***
  - **Nível das tabelas** – Privilégios de tabelas aplicam-se a todas as colunas em uma determinada tabela. **GRANT ALL ON db.tabela** e **REVOKE ALL ON db.tabela**
  - **Nível das colunas** – Privilégios de colunas aplicam-se a uma única coluna em uma determinada tabela **GRANT ALL (coluna1, coluna2) ON db.tabela**.

Concedendo Privilégios

```
mysql> GRANT privilegio [(colunas)] [, privilegio [(colunas)]] ...
    ON {*.* | db.* | db.tabela}
    TO usuario [IDENTIFIED BY 'senha'] [, usuario [IDENTIFIED BY 'senha']] ...
    [WITH [GRANT OPTION |
    MAX_QUERIES_PER_HOUR valor_limite |
    MAX_UPDATES_PER_HOUR valor_limite |
    MAX_CONNECTIONS_PER_HOUR valor_limite]]
```

Concedendo Privilégios

Concedendo o comando "**select**" para a tabela "**city**" dentro do BD "**bd2a14**" ao usuário "**taciano**":

```
mysql> GRANT select ON bd2a14.city TO 'taciano'@'localhost';
```

Concedendo o comando "**update**" para a tabela "**city**" dentro do BD "**bd2a14**" apenas na coluna "**population**" ao usuário "**taciano**":

```
mysql> GRANT update (population) ON bd2a14.city TO 'taciano'@'localhost';
```

Limpar o cache de privilégios:

```
mysql> FLUSH PRIVILEGES;
```

Concedendo Privilégios

Concedendo os comandos "**select, insert e update**" para qualquer tabela dentro do BD "**bd2a14**" ao usuário "**taciano**":

```
mysql> GRANT select, insert, update ON bd2a14.* TO 'taciano'@'localhost';
```

Concedendo **todos os privilégios** em todos os BDs e tabelas, com a possibilidade de **conceder privilégios** a outros usuários:

```
mysql> GRANT ALL ON *.* TO 'taciano'@'localhost' WITH GRANT OPTION;
```

Revogando Privilégios

```
mysql> REVOKE privilegio [(colunas)] [, privilegio [(colunas)]] ...
    ON {*.* | db.* | db.tabela}
    FROM usuario [, usuario ] ...
```

Revogando Privilégios

Revogando o comando "**select**" para a tabela "**city**" dentro do BD "**bd2a14**" ao usuário "**taciano**":

```
mysql> REVOKE select ON bd2a14.city FROM 'taciano'@'localhost';
```

Revogando o comando "**update**" para a tabela "**city**" dentro do BD "**bd2a14**" apenas na coluna "**population**" ao usuário "**taciano**":

```
mysql> REVOKE update (population) ON bd2a14.city FROM 'taciano'@'localhost';
```

Revogando Privilégios

Revogando os comandos "**select, insert e update**" para qualquer tabela dentro do BD "**bd2a14**" ao usuário "**taciano**":

```
mysql> REVOKE select, insert, update ON bd2a14.* FROM 'taciano'@'localhost';
```

Revogando o privilégios de **manipular todos os BDs e tabelas** e a possibilidade de **conceder privilégios** a outros usuários:

```
mysql> REVOKE ALL, GRANT OPTION FROM 'taciano'@'localhost';
```