

Sistemas de Informação  
**GSI016 Banco de Dados 1**



# SQL DCL e segurança

Prof. Humberto Luiz Razente  
humberto@facom.ufu.br  
Bloco B - sala 1B144

# Comandos para Controlar Relações - DCL

- ◆ CONNECT: Permite a conexão a uma base de dados através de um gerenciador
- ◆ DISCONNECT: Desconecta de uma base de dados
- ◆ COMMIT: Torna permanente todas as alterações feitas desde o início da conexão
- ◆ ROLLBACK: Descarta todas as alterações feitas desde o início da conexão, ou do último comando COMMIT ou ROLLBACK

# Segurança do Banco de Dados

◆ Os SGBD incluem recursos de segurança que controlam o modo como um banco de dados é acessado e usado

◆ Exemplo:

- Evitam o acesso ao BD sem autorização
- Controlam o uso de recursos do sistema (exemplo: tempo de CPU)
- Fazem auditoria das ações do usuário

# Mecanismos de Segurança

## ◆ Usuários e Esquemas do BD

- Cada BD tem uma lista de usuários, na qual cada usuário tem uma senha associada

## ◆ Domínio de Segurança

- São associados a cada usuário
- Conjunto de propriedades que determinam
  - ◆ Ações (privilégios e papéis) disponíveis

# Mecanismos de Segurança

## ◆ Privilégios

- Direito para executar um determinado tipo de declaração SQL
- Exemplos:
  - ◆ Direito de Conectar-se ao BD
  - ◆ Direito de criar uma tabela
  - ◆ Direito de selecionar linhas da tabela de outro usuário

# Mecanismos de Segurança

## ◆ Privilégios

- Atribuídos aos usuários finais
  - ◆ Exemplos:
    - ALTER: tabelas e sequências
    - DELETE: tabelas e visões
    - EXECUTE: procedimentos
    - Etc.

# Mecanismos de Segurança

## ◆ Concedendo Privilégios

- Duas formas

- ◆ **Explicitamente**

- Exemplo: o usuário Silva pode emitir comandos SELECT e INSERT, mas não DELETE usando a tabela EMPREGADO

- ◆ **Podem ser concedidos aos papéis** (um grupo nomeado de privilégios) que então são concedidos a um ou mais usuários

- Exemplo: o privilégio de emitir comandos SELECT e INSERT, mas não DELETE usando a tabela EMPREGADO pode ser concedido ao papel chamado GerenteRH, o qual pode ser concedido ao usuário Silva

# Mecanismos de Segurança

## ◆ Papéis

- São grupos de privilégios concedidos aos usuários ou a outros papéis
- Existem diversos papéis predefinidos
  - ◆ Exemplos: postgres, etc.



# Mecanismos de Segurança

## ◆ Papéis

### ■ Vantagens:

- ◆ Concessão reduzida de privilégios
  - Por grupos de usuários
- ◆ Gerenciamento dinâmico de privilégios
  - Se for necessários alterar privilégios de um grupo de usuários, altera-se apenas no papel
- ◆ Disponibilidade seletiva de privilégios
  - Permite o controle específico dos privilégios de um usuário em determinada situação

# O comando CREATE USER

- ◆ Permite a criação de novos usuários
- ◆ Sintaxe simplificada

```
CREATE USER username  
WITH 'password'
```

# Os comandos GRANT e REVOKE

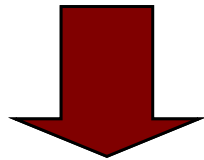
- ◆ GRANT : Permite atribuir privilégios
- ◆ REVOKE : Permite revogar privilégios
- ◆ Sintaxe simplificada para atribuir privilégios de sistema (pelo DBA)

```
GRANT {lista_privilégios | ALL [ PRIVILEGES ] }  
ON {lista_relações|lista_visões}  
TO {lista_usuários | papéis | PUBLIC}  
[WITH GRANT OPTION]
```

- WITH GRANT OPTION: permite que o usuário/papel que recebe o privilégio possa atribuí-lo a outros usuários

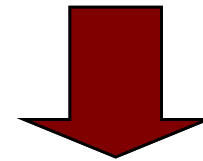
# GRANT e REVOKE

nível de conta



CREATE SCHEMA  
CREATE TABLE  
CREATE VIEW  
ALTER  
DROP  
MODIFY  
SELECT

nível de relação



SELECT  
UPDATE  
DELETE  
INSERT  
REFERENCES

# GRANT e REVOKE

## ◆ Particularidades

- o mesmo privilégio pode ser associado a um usuário  $U_1$  por qualquer número de outros usuários. Um comando REVOKE realizado por um usuário  $U_i$  somente remove os privilégios de  $U_1$  garantidos por  $U_i$
- um comando REVOKE realizado por um usuário  $U_i$  revoga todos os privilégios propagados a partir de  $U_i$  por meio da cláusula WITH GRANT OPTION

# O comando CREATE ROLE

- ◆ Permite criar novos papéis
- ◆ Sintaxe simplificada

```
CREATE ROLE role_name  
        PASSWORD 'password'
```

# Comandos adicionais

## ◆ Para excluir um papel

```
DROP ROLE role_name
```

## ◆ Para excluir um usuário

```
DROP USER username
```

## ◆ Para visualizar no dicionário de dados

### ■ Papéis, selecione a tabela

- ◆ pg\_roles

# Bibliografia

- ◆ Elmasri, Ramez; Navathe, Shamkant B. **Sistemas de banco de dados**. 4 ed. São Paulo: Addison Wesley, 2005, 724 p. Bibliografia: p. [690]-714.
- ◆ Deitel, H. M. **Java: como programar**. 6 ed. São Paulo: Pearson Prentice Hall, 2005.



# Leitura complementar para casa

## ◆ Elmasri – Navathe

- Capítulo 8

## ◆ Manual do SGBD PostgreSQL

- Explorar as outras particularidades dos comandos apresentados
- <http://www.postgresql.org/docs/manuals/>