



Laboratório de Bases de Dados

Prof. José Fernando Rodrigues Júnior

Aula 3 - Gerenciamento de Usuários e Privilégios

Material original editado: Profa. Elaine Parros Machado de Sousa



Conteúdo

- Gerenciamento de Usuários no Oracle
 - usuários
 - papéis (atribuições)
 - privilégios
- Revisão SQL/DML



Usuários

- Criação:

```
CREATE USER nome_usuario
  IDENTIFIED {BY senha | EXTERNALLY}
  DEFAULT TABLESPACE nome_tablespace
  TEMPORARY TABLESPACE nome_tablespace
  QUOTA {integer [K|M] | UNLIMITED} ON
                                     nome_tablespace

  PROFILE nome_profile
  PASSWORD EXPIRE
  ACCOUNT {LOCK | UNLOCK}
```



Usuários

- Exemplo:

```
CREATE USER labbd  
  IDENTIFIED BY labbd  
  DEFAULT TABLESPACE users  
  QUOTA 10M ON users  
  ACCOUNT UNLOCK
```



Usuários

- Exclusão:

```
DROP USER nome_usuario [CASCADE]
```



Privilégios

- **Privilégio** \Rightarrow autorização para que o usuário acesse e manipule objetos do BD.
- Tipos:
 - Sistema: permissão de executar ações no BD; DDL e gerenciamento
 - + de 100 tipos de privilégios distintos
 - ex: `create table, create session, create tablespace, create user, alter user, ...`
 - Objeto: permissão para acessar e manipular objetos específicos
 - ex: `select on Aluno, insert on Aluno, update (nusp) on Aluno ...`



Privilégios

- **Privilégios de sistema** – criação, alteração e remoção de objetos de esquemas
 - apenas em seu próprio esquema
 - ex: `create table, create view, create procedure, ...`
 - usuário é **dono** dos objetos que cria ⇒ possui permissão de alterar, remover, consultar, inserir, atualizar, executar, conceder privilégios sobre seus objetos, etc...
 - em qualquer (any) esquema - dado por usuário DBA
 - ex: `create any table, alter any table, drop any table, select any table, insert any table, execute any procedure ...`



Usuários

- Exemplo – privilégios de sistema:

Conectado como usuário dba:

```
GRANT CREATE SESSION, CREATE TABLE, CREATE  
SEQUENCE, CREATE SYNONYM TO labbd → apenas em  
seu próprio esquema
```

```
GRANT CREATE ANY TABLE, CREATE ANY SEQUENCE,  
CREATE ANY SYNONYM TO labbd → em qualquer  
esquema
```




Usuários

- Exemplo – privilégios de objeto:

Conectado como usuário teste:

```
GRANT SELECT,UPDATE ON F1 TO labbd;
```

```
GRANT UPDATE,DELETE ON F2 TO labbd;
```

```
GRANT REFERENCES ON F4 TO labbd;
```

```
GRANT ALL ON F5 TO labbd;
```

```
GRANT UPDATE (ARBITRO) ON F7 TO labbd;
```

```
GRANT INSERT (IDESTADIO, ESTADIO) ON F9 TO labbd;
```

```
GRANT REFERENCES (CAMPEONATO) ON F8 TO labbd;
```



Usuários

■ Ex

Co

GRAN

GRAN

GRAN

GRAN

GRAN

GRAN

GRAN

GRANT ALL se refere a:

**DELETE | INSERT | REFERENCES | SELECT | TRIGGER
| UPDATE**



Usuários

- Exemplo – privilégios de objeto:

Conectado como usuário labbd:

```
SELECT * FROM teste.F1;  
DELETE FROM teste.F2;  
UPDATE teste.F7 set ARBITRO = '';
```

Papéis (atribuições)

- **Papel:** grupo de privilégios

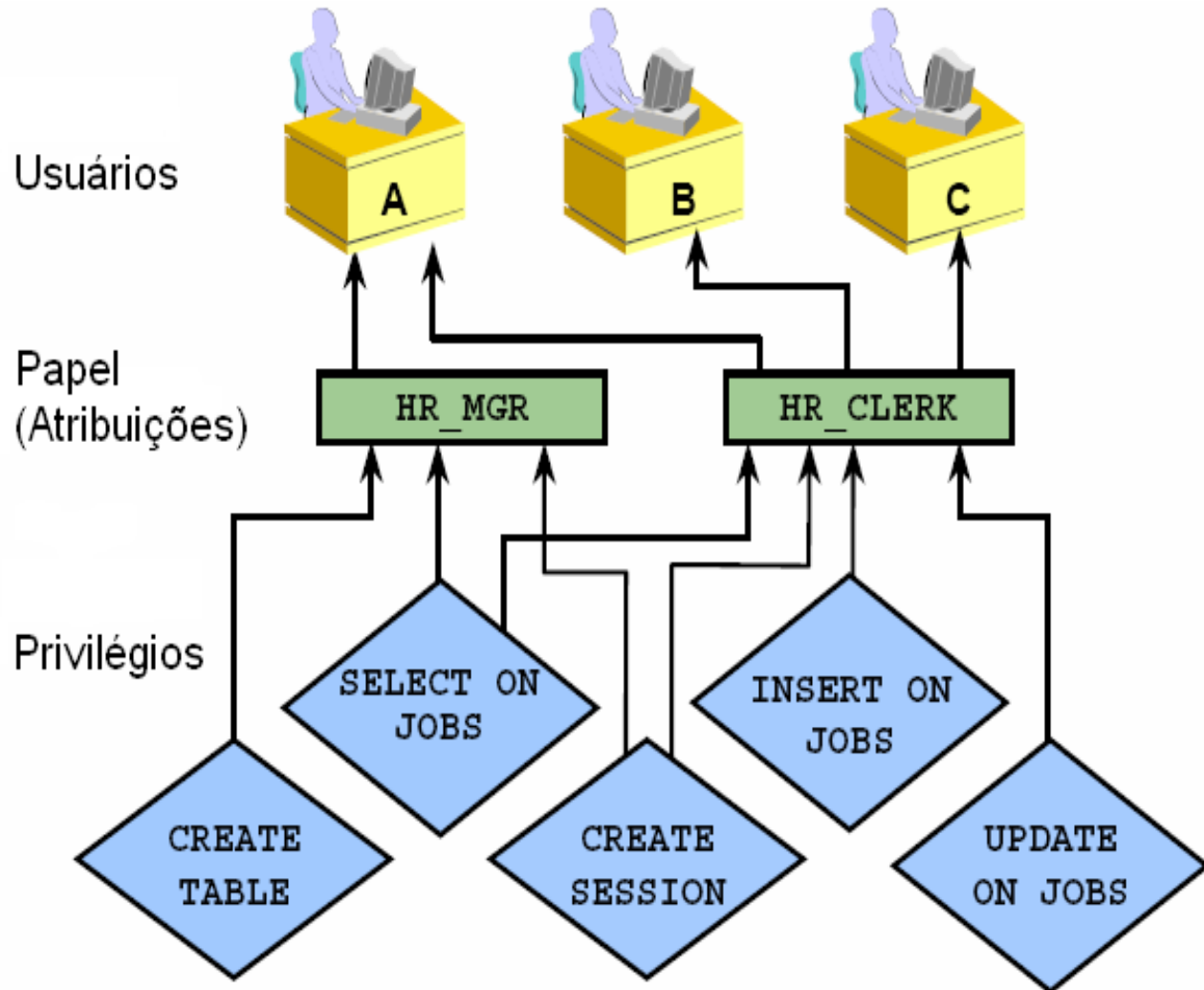
- simplifica a administração dos usuários

- Criar papel:

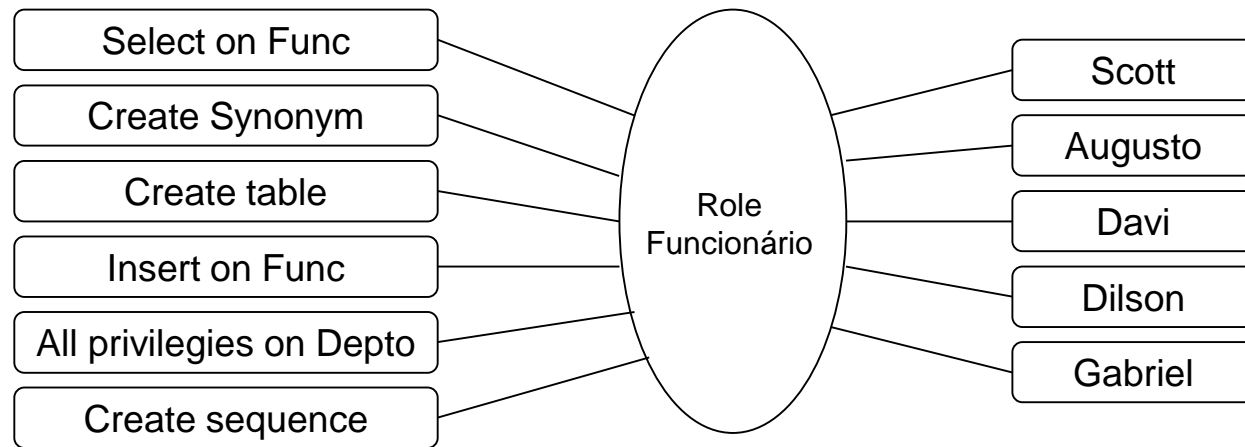
`CREATE ROLE papel`

- Excluir papel:

`DROP ROLE papel`



Exemplo



- Criar papel:

CREATE ROLE *FUNCIONARIO*;

- Atribuir alguns privilégios ao papel:

**GRANT CREATE SYNONYM, CREATE TABLE, CREATE SEQUENCE
TO FUNCIONARIO**

**GRANT SELECT ON FUNC, INSERT ON FUNC, ALL ON DEPTO
TO *FUNCIONARIO*;**

- Atribuir o papel ao usuário Scott:

**GRANT *FUNCIONARIO* TO Scott, Augusto, Davi, Dilson,
Gabriel;**



Privilégios, Papéis e Usuários

- Revogar privilégio e/ou papel:

```
REVOKE privilegio [,privilegio,...] | papel  
      [ON objeto]  
FROM usuario [,usuario,...] | papel
```

Exemplo:

dba: REVOKE CREATE TABLE FROM labbd;

teste: REVOKE SELECT ON F1 FROM labbd;



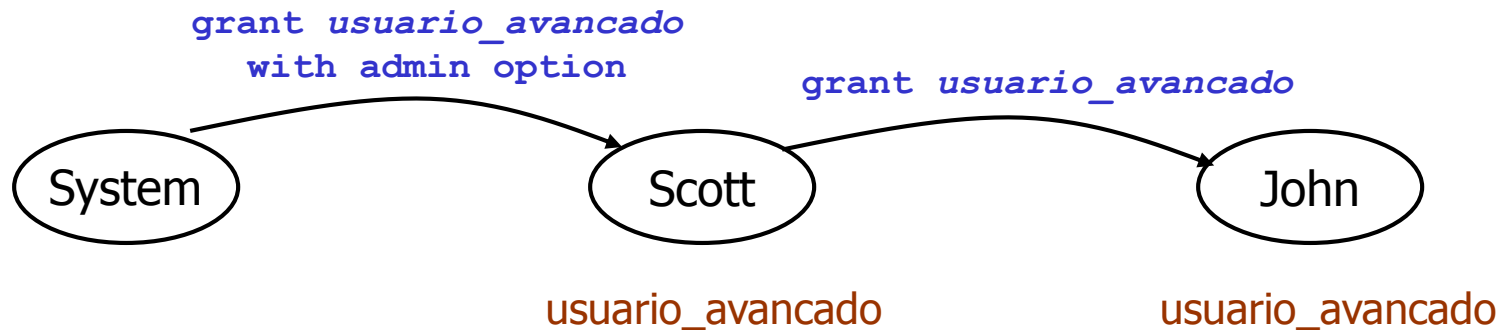
Privilégios, Papéis e Usuários

■ WITH ADMIN OPTION

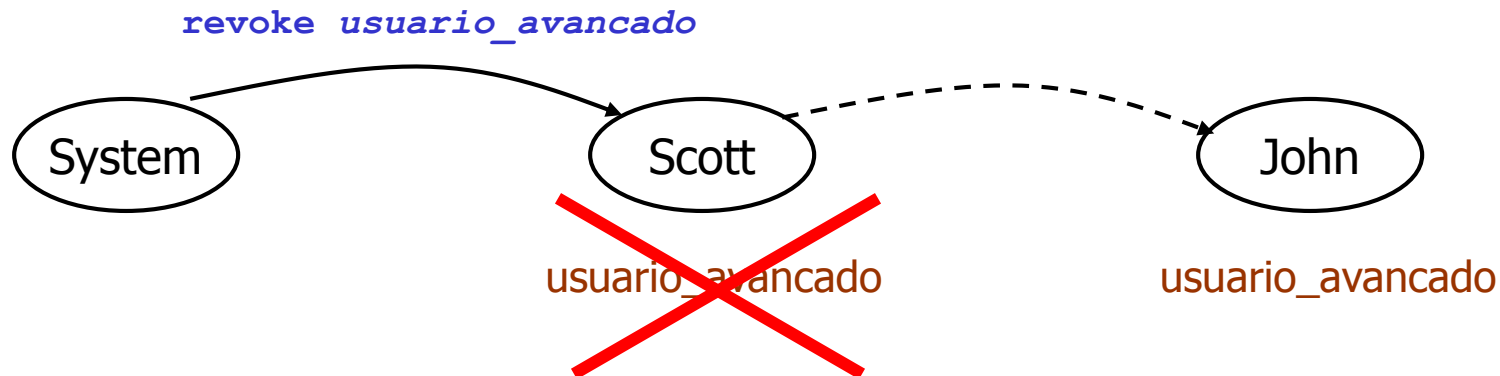
- opção para **privilégios de sistema**
- para usuários ou papéis
- permite ao usuário
 - conceder/revogar o privilégio/papel para/de qualquer usuário ou papel
 - alterar ou remover o papel concedido
- ex:

```
-- conectado como usuário dba
create role usuario_avancado;
grant create table to usuario_avancado;
grant usuario_avancado to Scott WITH ADMIN OPTION;

-- conectado como Scott
grant usuario_avancado to John;
```



```
-- conectado como usuário SYSTEM  
revoke usuario_avancado from Scott;
```





Privilégios, Papéis e Usuários

■ WITH GRANT OPTION

- opção para **privilégios de objetos**
- somente para usuários
- permite ao usuário
 - conceder o privilégio/papel para qualquer usuário (com ou sem **GRANT OPTION**) ou papel

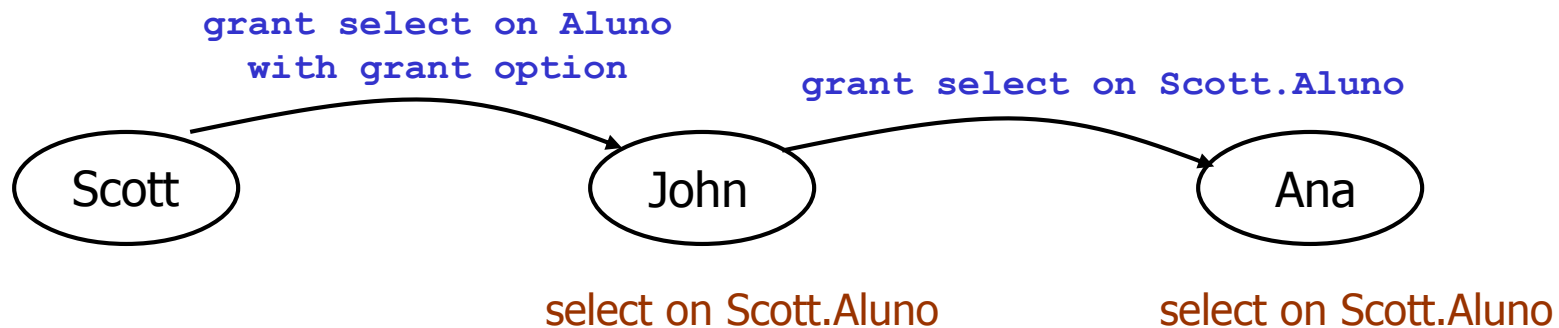
■ ex:

-- conectado como *Scott* (dono da tabela *Aluno*)

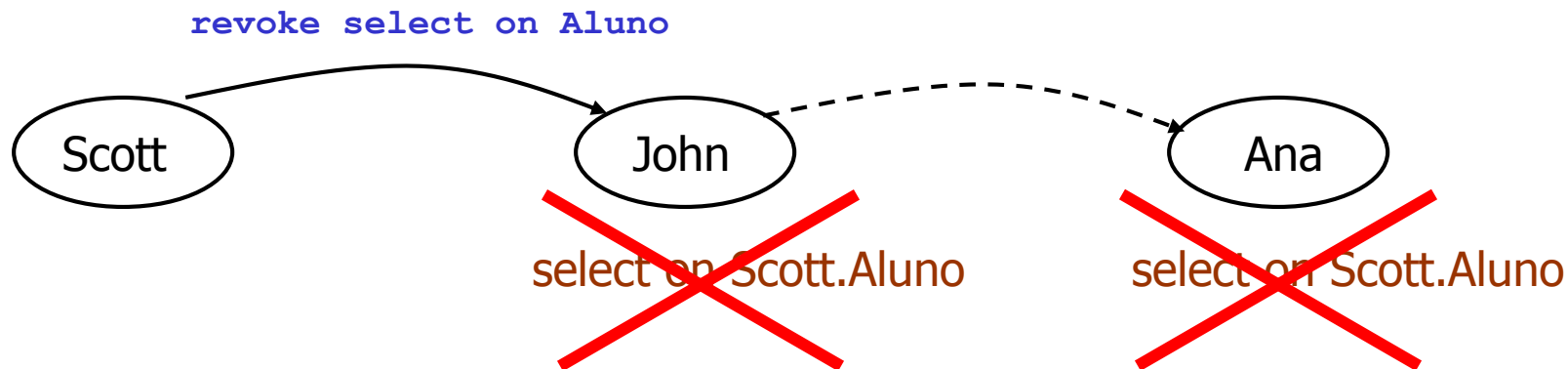
```
grant select on Aluno to John WITH GRANT OPTION;
```

-- conectado como *John*

```
grant select on Scott.Aluno to Ana;
```



```
-- conectado como usuário Scott  
revoke select on Aluno from John;
```



grant select on Aluno
with grant option

grant select on Scott.Aluno

No PostgreSQL, o REVOKE de objetos não é cascadeado.

~~select on Scott.Aluno~~

~~select on Scott.Aluno~~



Onde consultar ...

- Documentos em *list of books* no site da Oracle
 - Gerenciamento de Usuários
 - *Database Administrator's Guide*
 - *Database Security Guide*
 - *SQL Reference*
 - SQL/DML
 - *SQL Reference*
 - LOBs
 - *Application Developer's Guide - Large Objects (LOBs)*