SISTEMAS DE BANCO DE DADOS 2

AULA 6

Controle de Acesso (revisão)

MySQL

Vandor Roberto Vilardi Rissoli

APRESENTAÇÃO

- Controle de Acesso
- Usuários do Banco de Dados
- Privilégios de Acesso
- Papéis (e perfis) de Acesso
- Referências

Controle de Acesso

O termo **Controle de Acesso** é uma referência ao controle empregado para permitir ou não o acesso de pessoas a localidades (prédio, propriedade, sala, etc.), especialmente, se abordado sobre a segurança física.

"*Apenas as pessoas autorizadas têm acesso ao local*."

Aplicando o termo **Controle de Acesso** para segurança de dados o enfoque se mantém o mesmo, permitir ou não o acesso aos dados e informações armazenadas, sendo, geralmente, este controle formado pelos processos de:

i) **Autenticação**, *ii*) **Autorização**, *iii*) **Auditoria**

Controle de Acesso

AUTENTICAÇÃO: identifica quem acessa o sistema;

AUTORIZAÇÃO: determina o que um usuário autenticado pode fazer no sistema;

AUDITORIA: diz o que o usuário fez usando o sistema.

No contexto de **segurança dos dados**, o controle de acesso seria a habilidade de permitir ou negar o uso de um objeto (uma entidade passiva, como um sistema ou arquivo) por um sujeito (uma entidade ativa, como um indivíduo ou um processo).

Controle de Acesso

Um processo de dois passos identifica e autentica quem pode acessar o sistema e seus dados.

- Identifica quem é o usuário que está solicitando o acesso ao sistema (normalmente através do seu nome);
- Autentica a identidade do usuário verificando sua credencial, por exemplo, através de senha pessoal.

Com a evolução tecnológica, o reconhecimento por impressão digital, *smartcard*, face e outras tecnologias estão substituindo esse método de credencial (nome e senha), por exemplo, pela **biometria** se verifica características físicas e únicas de cada indivíduo.

Controle de Acesso

A autorização define quais direitos e permissões o usuário do sistema tem acesso, em que após sua autenticação a autorização determinará o que ele pode fazer ou visualizar no sistema.

Existem algumas **Técnicas de Controle de Acesso**, sendo três abordadas neste material:

- **Discricionário**: política de controle de acesso determinada pelo proprietário do recurso;
- **Obrigatório**: política de acesso é determinada pelo sistema e não pelo proprietário do recurso;
- **Baseado em Papéis**: abordagem que define os direitos e permissões baseados no papel que determinado usuário desempenha na empresa.

Controle de Acesso

- O controle **baseado em papéis** é uma abordagem para restringir o acesso aos usuários autorizados;
- Controles de acesso baseados em papéis (*roles*) definem os direitos e permissões baseados no papel que cada usuário realiza na organização;
- Esta estratégia simplifica o gerenciamento das permissões dadas aos usuários e pode constituir **perfis** comuns entre os usuários e sua atribulações;
- Permissões de acesso e direitos sobre objetos são dados para qualquer grupo ou indivíduos, em adição;
- Os indivíduos podem pertencer a um ou mais grupos, adquirir permissões cumulativas ou retirar qualquer permissão que não faz parte de todo seu grupo.

Usuários

A linguagem SQL também trabalha no Controle de Acesso, criando usuários e fornecendo os privilégios correspondentes às necessidades de seus diferentes usuários.

Sintaxe geral para criação de usuário em SQL:

```
CREATE USER <<nomeUsuario>>
   IDENTIFIED {BY <<senha>> | EXTERNALLY}
   DEFAULT TABLESPACE <<nomeTablespace>>
   TEMPORARY TABLESPACE <<nomeTablespace>>
   QUOTA {integer [K|M] | UNLIMITED} ON  <<nomeTablespace>>
   PROFILE <<nomeProfile>>
   PASSWORD EXPIRE
   ACCOUNT {LOCK | UNLOCK}
```

Usuários

Exemplo:

```
CREATE USER maria
    IDENTIFIED BY airam321
    DEFAULT TABLESPACE users
    TEMPORARY TABLESPACE users
    QUOTA 10M ON users
    ACCOUNT UNLOCK;
```

Usuários

REMOVENDO USUÁRIO

A instrução SQL que remove um usuário do banco de dados consiste em:

DROP **USER** **<<nomeUsuario>>** **;**

Exemplo:

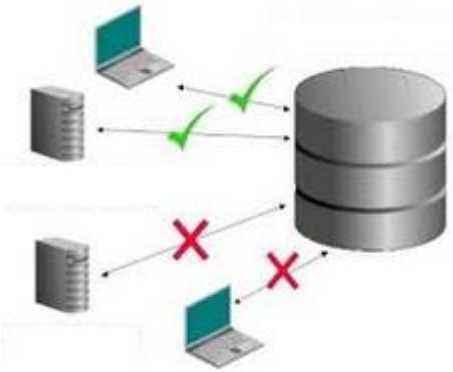
DROP **USER** **maria** **;**

De acordo com o **Sistema Operacional** que o SGBD estiver funcionando, deverá se ter o cuidado com maiúsculo e minúsculo, sendo sugerido sempre respeitá-los então.

Privilégios

Os usuários do SGBD são **diferentes** dos usuários gerenciados pelo Sistema Operacional, em que o SGBD executa.

Todo SGBD possui um conjunto de usuários que se utilizam de seus dados e recursos, conforme tenham autorização e permissões concedidas através de privilégios para usufruírem dos recursos e/ou conteúdos armazenados no SGBD.



Privilégios

- **PRIVILÉGIO** $\Rightarrow$ autorização fornecida para o usuário do SGBD para acessar e/ou manipular recursos, estruturas e dados armazenados.

- **TIPOS** DE RECURSO DO SGBD
  - SISTEMA
    - Permissão de executar ações sobre o SGBD, seus objetos e estruturas (vários tipos de privilégios distintos);
  - OBJETO
    - Permissão para acessar e manipular um objeto ou estrutura específica (os dados armazenados).

Privilégios

SISTEMA

- CREATE TABLE
- CREATE USER
- ALTER TABLE
- DROP USER
- entre outros (mais de cem tipos)

OBJETO

- SELECT
- INSERT
- UPDATE
- DELETE
- e outros, sendo estes quatro os principais

O usuário é **dono** dos objetos que cria, tendo todos os privilégios sobre ele, além de poder conceder privilégios para outros usuários sobre os seus objetos.

Privilégios

Alguns SGBD permitem agrupar privilégios, formando **perfis** característicos de acesso em um Projeto de Banco de Dados e depois associar os usuários aos seus respectivos perfis, por exemplo:

- **ORACLE**: cria **ROLE** que recebe privilégios e forma perfis de acesso que podem ser melhor geridos pelos profissionais de BD, por exemplo, DBA;

- **PostgreSQL**: similar ao ORACLE (ROLE) este SGBD também cria perfis e depois vincula os usuários a cada perfil, por meio de um objeto denominado **GROUP**;

- **MySQL**: não possui este recurso até a versão 5, mas investigar.

Verificar na versão 8 do MySQL

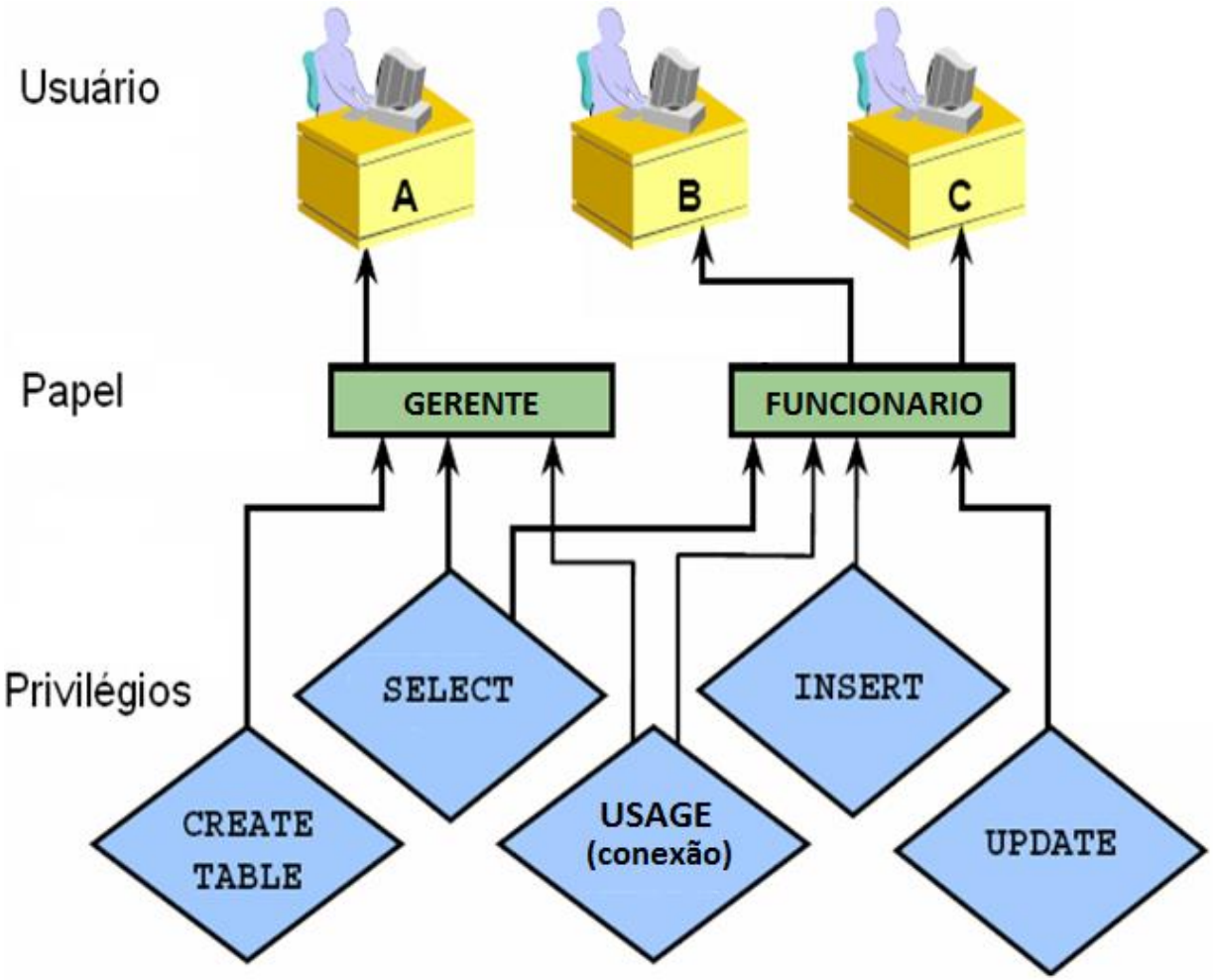
Papéis (atribuições)

- **Papel:** agrupa privilégios
  - simplifica a administração dos usuários
- Criar Papel (perfil)

```
CREATE ROLE papel
```

- Excluir Papel

```
DROP ROLE papel
```



Papéis (atribuições)

As atribuições de privilégios podem acontecer diretamente para usuários ou aos papéis (perfis), que posteriormente terão os usuários associados, fornecendo lhes os respectivos privilégios concedidos ao perfil.

- Concessão de privilégios
  - de **SISTEMA**

    GRANT *privilegio* [, *privilegio*,...] | *papel*
    TO *usuario* [, *usuario*,...] | *papel* | PUBLIC
    [WITH **ADMIN** OPTION]

  - de **OBJETO**

    GRANT *privilegio* [, *privilegio*,...] | *papel* **ON** *objeto*
    TO *usuario* [, *usuario*,...] | *papel* | PUBLIC
    [WITH **GRANT** OPTION]

Papéis (atribuições)

REMOVENDO PRIVILÉGIO

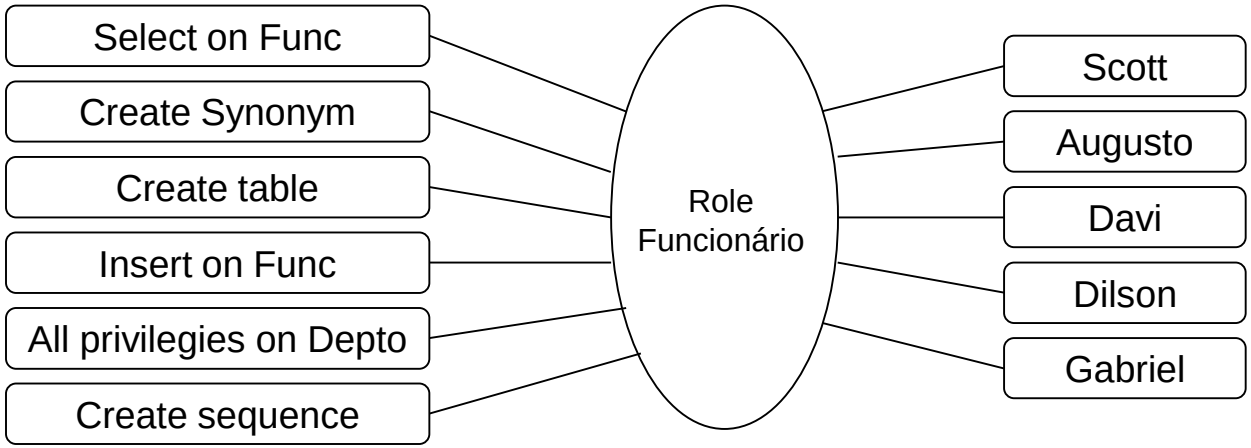
É possível remover qualquer privilégio de um usuário, sendo comprometida para ele as ações que anteriormente podia realizar no SGBD.

- Remover ou revogar privilégio

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

A instrução **REVOKE** revoga os privilégios de SISTEMA ou de OBJETO.

Papéis (atribuições)



Exemplos:

- Atribuir alguns privilégios para usuário Davi:

  GRANT CREATE TABLE, CREATE VIEW TO DAVI;

  GRANT SELECT, INSERT ON TABELA_FUNC TO DAVI;

- Trabalhando com Papéis para usuário Dilson:

  CREATE ROLE FUNCIONARIO; (atribuir privilégios ao perfil)

  GRANT FUNCIONARIO TO DILSON;

Papéis (atribuições)

CONCEDENDO PRIVILÉGIOS

A atribuição de um privilégio para outro usuário pode permitir que este novo usuário com privilégio possa repassá-lo para outros usuários.

- **WITH ADMIN OPTION**
  - Opção para **privilégios de sistema**
  - Pode ser concedida para usuários ou papéis (perfis)
  - permite ao usuário
    - Conceder ou revogar o privilégio de qualquer usuário ou papel;
    - Alterar ou remover o papel concedido.

Papéis (atribuições)

Exemplo:

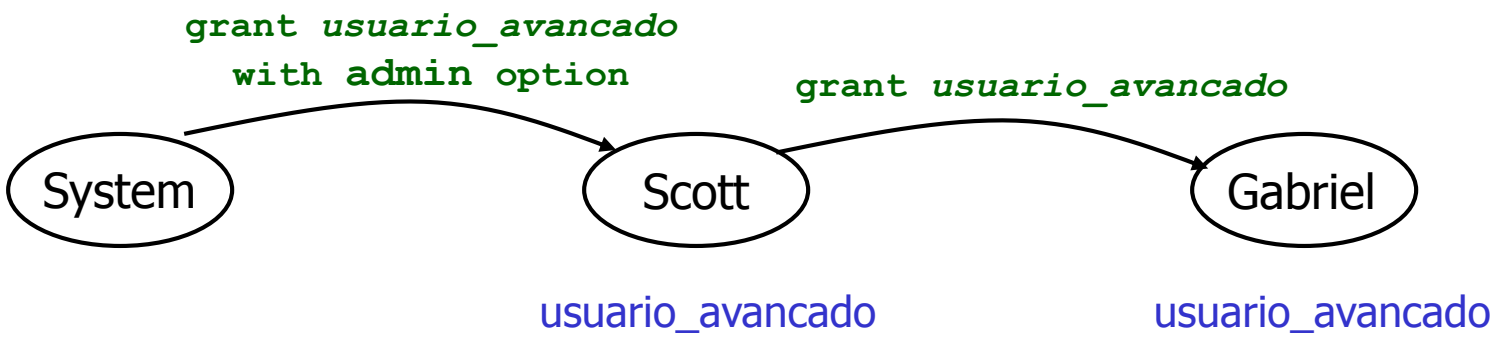
- Conectado como superusuário do SGBD (***root***)

```
CREATE ROLE usuario_avancado;
GRANT create table TO usuario_avancado;
GRANT usuario_avancado TO SCOTT
    WITH ADMIN OPTION;
```

- Conectado como **SCOTT**

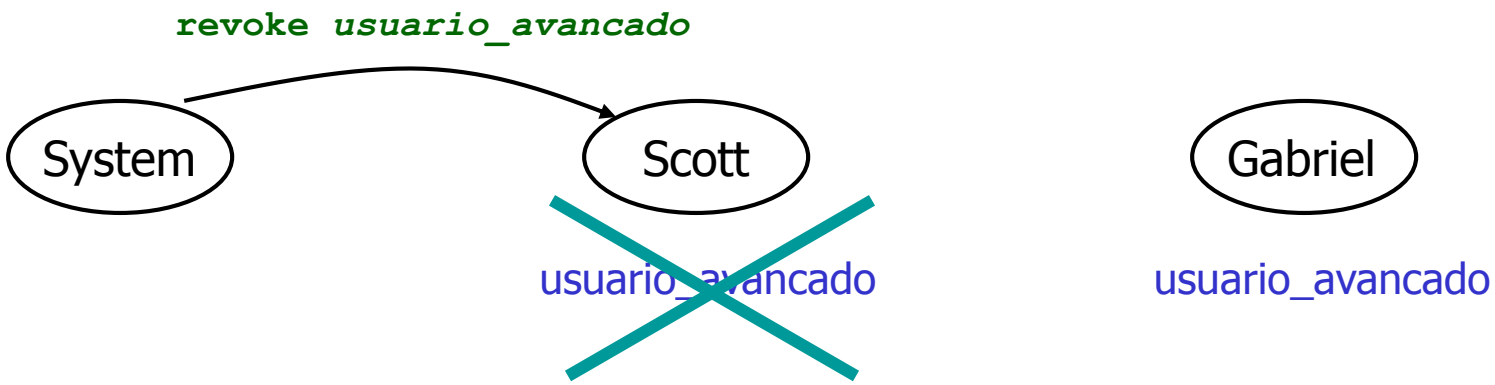
```
GRANT usuario_avancado TO GABRIEL;    ( ou )
GRANT create table TO GABRIEL;
```

Papéis (atribuições)



Conectado como superusuário (*root*)

```
REVOKE usuario_avancado FROM SCOTT;
```



Papéis (atribuições)

- **WITH ADMIN OPTION**
  - Opção para **privilégios de Objetos**
  - Fornecida somente para Usuários
  - permite ao usuário
    - Conceder o privilégio para qualquer usuário (com ou sem **Grant Option**) ou papel;
    - Alterar ou remover o papel concedido.

Exemplos:

- Conectado como *Scott* (é o dono da tabela ALUNO)

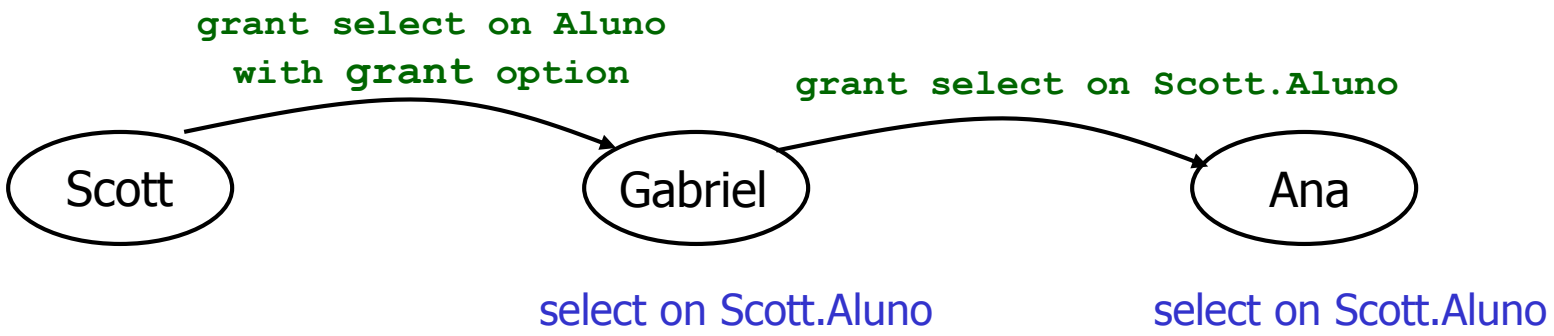
  GRANT select ON ALUNO TO *DAVI*

  WITH GRANT OPTION;

- Conectado como *Davi*

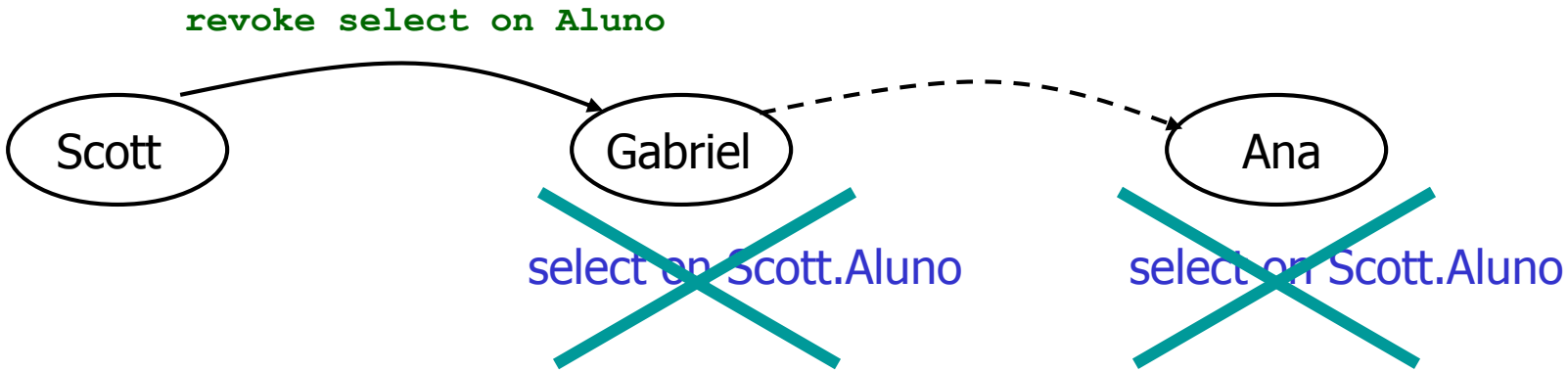
  GRANT select ON SCOTT.ALUNO TO DILSON;

Papéis (atribuições)



Conectado como usuário Scott

```
REVOKE select ON ALUNO FROM JOHN;
```



Papéis (atribuições)

Como acontecem os efeitos após a execução das instruções GRANT e REVOKE no SGBD?

- Privilégios (de SISTEMA e de OBJETOS) para usuários e papéis
  - efeito IMEDIATO para as sessões correntes e sessões posteriores (novas);

- Papéis para usuários e papéis
  - sessões posteriores ⇒ efeito IMEDIATO
  - sessões correntes ⇒ necessidade de instruções para reabilitar o papel

MySQL FLUSH PRIVILEGES;

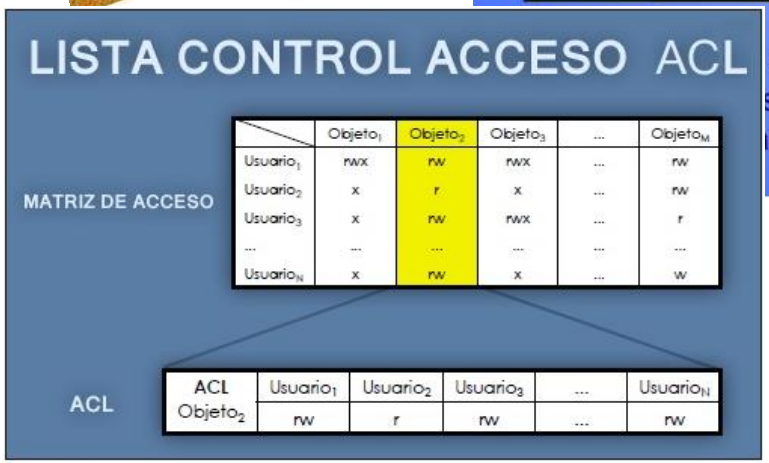
ORACLE SET ROLE

Papéis (atribuições)

Algumas indicações de formulários para representação do gerenciamento do controle de acesso.

Permissões de Acesso	AdminApp	Grupos UserApp	UserAppBD
Perfil de Grupo	Concedido	Negado	Negado
Atribuir Membros	Concedido	Negado	Negado
Apagar	Concedido	Negado	Negado
Gerir Anúncios	Concedido	Negado	Negado
Permissões	Concedido	Negado	Negado
Gerir Páginas	Concedido	Negado	Negado
Atualizar	Concedido	Negado	Concedido
Visualizar	Concedido	Concedido	Concedido

	Archivo1	Archivo2	Archivo3	D1	D2	D3
D1	Leer Escribir		Ejecutar		Entrar	
D2	Leer	Leer Escribir		Entrar		Entrar
D3		Escribir	Ejecutar Leer			



TIPO	GRUPO	MEMBROS
User Roles	IDM USER TODOS	Todos os colaboradores
	IDM USER CC 1234	Todos os colaboradores do centro de custo 1234
	IDM USER CC 1235	Todos os colaboradores do centro de custo 1235
	IDM USER CC 1236	Todos os colaboradores do centro de custo 1236
	IDM USER VINCULO FUNCIONARIOS	Todos os colaboradores que são funcionários
	IDM USER VINCULO TERCEIROS	Todos os colaboradores que são terceiros
Application Roles	IDM APPL AUTO ADMIN	[IDM USER CC 1234]
	IDM APPL BLOQUEIO ADMIN	[IDM USER VINCULO TERCEIROS]
		João Ninguém
	IDM APPL MANUAL ADMIN	Ticiano Benetti
	IDM APPL AUTO USUARIOS	[IDM USER TODOS]
	IDM APPL BLOQUEIO USUARIOS	[IDM USER VINCULO TERCEIROS]
	IDM APPL MANUAL USUARIOS	

Exercícios de Fixação

1) Com o objetivo de integrar um novo artefato no projeto, mas como um documento significativo a compreensão lógica das atribuições de privilégios para cada perfil relevante do Exercício 1 da Aula 3 (***Plantonistas***), elabore um diagrama, tabela ou outro recurso que após uma pesquisa você acredite ser mais esclarecedor aos envolvidos no projeto e que não compreende o *script* **Controle** em SQL.

3 Perfis são bem definidos ao uso da BD do projeto:

administrador: corresponderá ao DBA do projeto;

gestor: responsável pela gestão dos plantonistas;

usuario: qualquer pessoa que use o hospital.

Exercícios de Fixação

Continuação do exercício 1:

Definições para os 3 perfis do projeto:

administrador: possui todos os privilégios sobre essa base de dados somente, pois será o DBA para administrar essa BD (base de dados), além de poder repassar os seus privilégios para outros usuários;

gestor: possui privilégios de consultar todas tabelas dessa BD, mas também poderá **cadastrar** e **alterar** dados do **plantonista** e do **setor** do hospital;

usuario: possui somente o privilégio de **consultar** todos os dados somente dessa BD.

Referência de Criação e Apoio ao Estudo

Material para Consulta e Apoio ao Conteúdo

- ELMASRI, R.; NAVATHE, S. B. Sistemas de Banco de Dados. 4ª ed. 2005
  - Capítulo 23
- DEVMEDIA - Gerenciamento de Usuários e Controle de Acessos do MySQL
  - http://www.devmedia.com.br/gerenciamento-de-usuarios-e-controle-de-acessos-do-mysql/1898
- XOOPS Brasil - Segurança Geral
  - https://xoops.net.br/docs/mysql/manual/ch04s03.php