Sistema de Gestão de Bases de dados

- **ISUTC** INSTITUTO **SUPERIOR** DE **TRANSPORTES** E **COMUNICAÇÕES**

O Grupo da Disciplina

DEPARTAMENTO DE TECN. DA INFORMAÇÃO E COMUNICAÇÃO

Ano Lectivo 2024

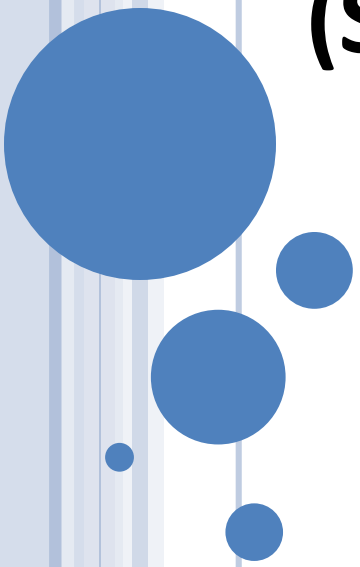
Base de Dados

1° semestre

CONTEÚDO

- **Protecção de dados e Gestão de Usuários:**
  - Tipos de segurança;
  - Autenticação e Controlo de acessos;
  - Privilégios, Roles
  - **Actividades práticas 23 e 24 (TPC)**

SQL
(Structured Query Language)



Segurança de base de dados

Introdução

A segurança em BDs, como em qualquer sistema, é fundamental para qualquer organização que armazene informações sensíveis. Com o aumento constante das ameaças, é essencial adoptar medidas de segurança robustas em bancos de dados MySQL de modo a assegurar a proteção e gestão de seus activos.

Tipos de Segurança

- Segurança de Rede – gestão de tráfego de dados através de uso de firewalls.
- Proteção de Informação – através de criptografias; backups e restauração; e segurança física.
- Proteção contra ameaças – auditoria e detenção de ameaças.
- Gestão de Acessos.

Administração de Acessos em BDs no MySQL

- O papel do administrador da BD é crucial em qualquer SGBD. É ele que atribui e restringe permissões.
- Este deve ter muito cuidado ao atribuir um conjunto de permições a um utlizador, garantindo a protecção dos dados e negação de acessos não autorizados.
- Cabe portanto ao DBA criar os utilizadores que poderão usar o MySQL, podendo também renomeá-los e removê-los permanentemente do SGBD.
- Assim que o MySQL inicializa ele tem por defeito o user root, acedido com a senha pré-definida na instalação.

Para visualizar o user e sua localização usa-se o comando:

Select user, host from mysql.user;

Passos para Criação de users e concessão de previlégios no MySQL

1. Aceder a linha de comando e entrar no servidor MySQL;
2. Autenticar a inicialização do MySQL;
3. Criação de novo user e sua senha;
4. Concessão de previlégios/Permissões;
5. Ajuste de previlégios/Permissões;
6. Consulta de usuários;
7. Exclusão de usuários.

- A sintaxe para criar um usuário é:

```
CREATE USER usuario@host [IDENTIFIED BY[PASSWORD]]
'senha';
```

- Onde:

usuario representa o nome do usuário que será criado;

'senha' representa a senha de acesso ao MySQL pelo usuário criado.

Ex: **Create user Gilda@localhost IDENTIFIED BY '12345';**

Depois de criarmos um usuário com senha no MySQL, temos a possibilidade de alterarmos a senha desse usuário, conforme a sintaxe:

SET PASSWORD FOR usuario PASSWORD ('nova senha')

Renomeação ou exclusão de usuários

- Um user a semelhança de outros objectos, pode ser alterado, renomeado ou apagado a partir dos comando DDL.

- Ex:

  Rename Gilda To GildaMuhai;

  Drop user GildaMuhai;

Concessão de privilégios/Permissões

O MySQL concede os privilégios de acordo com a identidade e com o que se deseja fazer no SGBD.

A administração de permissões num SGBD é efectuada através das instruções DCL – Data Control Language

- GRANT - Atribuição de permissões.
- REVOKE - Remoção de permissões

Para a concessão de permissãoes é necessário que o utilizador que atribui as permissões:

- ✓ Seja o dono do objecto;
- ✓ Possua permissões de nível máximo;
- ✓ A permissão sobre o objecto lhe tenha sido atribuída com a clausula **“WITH GRANT OPTION”** .

Tipos de Privilégios

Existem diferentes tipos de privilégios passíveis de atribuição/remoção, sendo alguns específicos de cada SGBD:

- Tabela - Controlo sobre os utilizadores que podem aceder ou modificar a informação contida numa tabela.
- Objecto da BD - Controlo sobre os utilizadores que podem criar ou remover objectos da base de dados (funções, procedimentos, vistas, ...).
- Sistema - Controlo sobre os utilizadores com permissões para executar tarefas de administração de sistema (REORG, ...).
- Stored Procedures - especificação dos utilizadores que podem executar procedimentos ou funções guardadas no SGBD.

- Comando para concessão de Previlégios

```
GRANT priv [(colunas)] [, priv [(colunas)]] ...
ON {*.* | db.* | db.tabela}
TO usuario [IDENTIFIED BY 'senha']
[, usuario [IDENTIFIED BY 'senha']] ...
```

Ex:

GRANT ALL ON estudante TO Gilda;

Para visualizar os previlégios atribuidos:

SHOW GRANTS FOR usuario;

Previlégios de Tabela

- SELECT - Permissão para o utilizador consultar consultar informação de uma tabela ou vista.

Ex:

GRANT **SELECT** (nome, idade) ON estudante TO Gilda;

- INSERT - Permissão para o utilizador inserir novas instâncias numa tabela.

Ex:

GRANT **INSERT** ON estudante TO Gilda;

- UPDATE - permissão para o utilizador alterar informação da tabela.

Ex:

GRANT **UPDATE** ON estudante TO Gilda;

- DELETE - Permissão para o utilizador eliminar instâncias de uma tabela de uma tabela

Ex:

GRANT **DELETE** ON estudante TO Gilda;

- ALL - Conjunto de todas as permissões anteriores.

Previlégios de Objectos

- Permite a criação de cada um dos tipos disponibilizados pelo SGBD (bases de dados, tablespaces, índices, eventos, tipos,...).

Ex:

GRANT trigger, index TO Gilda;

Previlégios de Sistema

- Define os utilizadores que podem executar comandos SQL específicos (criação de ficheiros de log, desactivação de bases de dados, monitorização de performance, criação de backups,...)
  - Não são atribuídos ao nível da base de dados Não são atribuídos ao nível da base de dados;
  - Varia bastante enter SGBD´s.
- Ex: GRANT TRACE TO Utilizador1;

Permite que o “utilizador1” possa efectuar a análise do caminho para os dados de determinadas consultas.

Previlégios de Stored Procedures

- Privilégios de execução - Permitem definir quais os utilizadores que podem executar que funções e podem executar que funções e procedimentos guardados no SGBD.

- Ex: GRANT EXECUTE ON PROCEDURE mydb.myproc TO Gilda;
- Permite que “n” utilizadores executem o procedimento “procedure1 ”

Privilégios públicos

- É possível a atribuição de privilégios a todos os utilizadores de um SGBD os utilizadores de um SGBD.
- Não pode ser conjugado com a clausula “WITH GRANT OPTION” – Indicada para os recursos que devam estar Indicada para os recursos que devam estar disponíveis para todos os utilizadores. – Pode implicar falhas ao nível da fiabilidade da informação.
- Ex:
- GRANT DELETE ON Pessoas TO PUBLIC Permite que qualquer utilizador possa eliminar instâncias da tabela “Pessoas”

Remoção de privilégios

- Constituí a instrução “simétrica” de “GRANT”. Possui sintaxe exactamente igual ao GRANT.
- Ex: – REVOKE UPDATE ON Pessoas (Nome) To Utilizador1

Retira o privilégio de alteração do atributo “Nome”da tabela “Pessoas” ao “Utilizador1”.

A remoção de privilégios com a clausula “PUBLIC” não retira aos utilizadores cuja atribuição tenha sido feita especificamente. – A remoção de objectos de uma base de dados implica automaticamente a remoção de todos os privilégios atribuídos sobre ele.

Remoção de privilégios

- Comando de Remoção de Previlégios:

REVOKE priv [(colunas)] [, priv [(colunas)]] ...
ON {*.* | db.* | db.tabela}
FROM usuario [, usuario] ...

Ex:

REVOKE SELECT ON estudantes FROM Gilda;

REVOKE all, grant option FROM Gilda;

Verificação

- Para se certificar de que os previlégios foram carregados executa-se o omando:

  FLUSH PRIVILEGES;

Roles

Roles ou papeis em português.

- Por forma a facilitar as tarefas de administração de privilégios é possível: administração de privilégios, é possível:
  - Criar regras que contenham um conjunto de privilégios.
- Ex:

```
CREATE role MANAGER;
GRANT SELECT ON Tabela1 TO MANAGER;
GRANT UPDATE ON Tabela2 TO MANAGER;
COMMIT;
GRANT MANAGER TO Utilizador1;
```

Permite atribuir 2 regras (selecção e alteração) ao “Utilizador1” numa só instrução.

ACTIVIDADE 23

1. Crie diferentes tipos de utilizadores da BD da actividade2:
   - Um user que tem permissões de consulta penas;
   - Um user que para além de consultas pode actualizar os dados na BD;
   - Um user admin para gerir a BD.
2. Faça acessos a partir dos users acima e de acordo com os privilégios:
   - Faça uma inserção na tabela compra;
   - Liste as compras efectuadas;
   - Crie um procedimento armazenado lista a compra efectuada sempre que se efectuar.
3. Crie uma *view* a ser usada pelo utilizador com permissões de consulta que lista os itens comprados.

ACTIVIDADE 24

4. Um DBA executou os seguintes comandos em um SGBD relacional, onde se encontra uma BD com duas tabelas, tbl_funcionário e tbl_departamento, e os usuários, Gilda, Duarte e Nelton:

- grant select, update on tbl_departamento to Gilda, Duarte with grant option;
- grant select, update on tbl_funcionário to Gilda, Duarte with grant option;
- grant delete, insert on tbl_departamento to Duarte, Nelton;

Depois, o seguinte commando foi efectuado pelo usuário user2 (Duarte):

– grant update on tbl_departamento to Nelton;

Por fim, o DBA executou o comando

– revoke select, update on tbl_departamento from Duarte;

Num cenário válido, após a execução dos comandos acima, o usuário:

a) Gilda possuirá direito de leitura e inserção na tabela tbl_funcionario;
b) Gilda possuirá direito de remoção e actualização na tabela tbl_departamento;
c) Duarte possuirá direito de leitura e inserção na tabela tbl_funcionario;
d) Nelton possuirá direito de remoção e inserção na ybl_funcionario;
e) Nelton possuirá direito de remoção e inserção na tbl_departamento.

GARANTE O TEU FUTURO

COM UMA FORMAÇÃO SÓLIDA

ISUTC

Prolong. da Av. Kim Il Sung (IFT/TDM) Edifício D1
Maputo, Moçambique

www.facebook.com/isutc

www.transcom.co.mz/isutc