



Aula

Aspectos de Segurança em Banco de
Dados

13

Controle de

Redundância

planejamen/o e

Controle de Redundância

Definição

O redundância consiste no armazenamento de uma mesma informação em locais diferentes, provocando inconsistências. **Em um Banco de Dados as informações só se encontram armazenadas em um único local, não existindo duplicação descontrolada dos dados.** Quando existem replicações dos dados, estas são decorrentes do processo de armazenagem típica do ambiente Cliente-Servidor, totalmente sob controle do Banco de Dados.

A aplicação da Normalização e das Formas Normais tem como um dos objetivos a eliminação da redundância de dados.

Controle de Redundância

- A redundância é caracterizada pela presença de um elemento de informação duplicado.
- Sistemas de banco de dados devem ter capacidade de garantir que os dados não sejam redundantes.
- Esse controle é usualmente conhecido como integridade referencial.
- O controle de redundância não permite incluir dois registros com a mesma chave primária e excluir um registro que possua relacionamento com outras tabelas (chave estrangeira).
- Com isto, o controle de redundância evita a inconsistência de dados.
- Este padrão de integridade é o fundamento do modelo relacional, por isso é necessário que o banco de dados tenha a capacidade

Controle de

Concorrência

planejamen/o e

Controle de Concorrência

Definição

É necessário que o sistema controle a interação entre transações concorrentes. Esse controle é alcançado por meio de uma larga gama de mecanismos chamados **esquemas de controle de concorrência.**

Existem vários esquemas de controle de concorrência onde um dos mais conhecidos é o esquema que tem por base a propriedade de serialização.

Controle de Concorrência

Definição

O Controle de Concorrência tem como principal objetivo o **evitar conflitos de acesso simultâneo.**



PC-2 é bloqueado porque PC-1 fez a mesma solicitação antes e SGBD ainda está executando

Restrições de

Integridade

planejamen/o e

Restrições de Integridade

Definição

Verifica em toda transação se os tipos de dados estão corretos, por exemplo, impede que seja armazenado uma data onde espera-se um número.

Cliente	
nome: VARCHAR (30)	idade: INT(3)
João	12
Carlos	20
Renata	17

Ao projetar o banco de dados você deve se preocupar com as Restrições de Integridade, por exemplo, se um usuário tentar executar o comando:

```
INSERT INTO cliente(nome, idade)  
VALUES('Talia', '1984/02/01');
```

O banco deve retornar um ERRO para o usuário e informar qual o erro e como corrigi-lo, mesmo que seja óbvio para quem projetou o sistema.

Violação e Consistência dos

Dados *planejamen/o e* *segurança...*

Violação e Consistência dos Dados

Definição

Para evitar a violação dos dados e garantir a consistência, confiabilidade, podemos adotar alguns mecanismos de segurança entre esses mecanismos podemos destacar:

- **Mecanismos de Controles Físicos**

Portas / Trancas / Paredes / Blindagem / etc...

- **Mecanismos de Controles Lógicos**

Mecanismos de criptografia / Assinatura digital / Mecanismos de garantia da integridade da informação / Mecanismos de controle de acesso / etc...

Violação e Consistência dos Dados

Criptografi

a Criptografia, considerada como a ciência e a **arte de escrever mensagens em forma cifrada ou em código**, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet. A primeira vista ela até pode parecer complicada, mas para usufruir dos benefícios que proporciona você não precisa estudá-la profundamente e nem ser nenhum matemático experiente. Atualmente, a criptografia já está integrada ou pode ser facilmente adicionada à grande maioria dos sistemas operacionais e aplicativos e para usá-la, muitas vezes, basta a realização de algumas configurações ou cliques de mouse.

Violação e Consistência dos

Dados

Assinatura

Digital

A Assinatura Digital **permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada.**

A assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia ter feito isto. A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo. Para contornar a baixa eficiência característica da criptografia de chaves assimétricas, a codificação é feita sobre o hash e não sobre o conteúdo em si, pois é mais rápido codificar o hash (que possui tamanho fixo e reduzido) do que a informação toda.


SQL

Injection

planeiamen/o e

SQL Injection

Definição

 de SQL, mais conhecida através do termo SQL Injection, é um tipo de segurança que acontece devido a falhas em sistemas que interagem com bases de dados via SQL. A injeção de SQL **ocorre quando o atacante consegue inserir uma série de instruções SQL dentro de uma consulta (query) através da manipulação das entradas de dados de uma aplicação.**

SQL

Injection

Definição

Q Para que se esteja livre da utilização da SQL Injection, certas providências devem ser tomadas. Algumas das ações serão realizadas no servidor de banco de dados, outras devem ser garantidas pelo código fonte.

- Deve-se tomar cuidado com a configuração do usuário que estabelece a conexão com o banco de dados.
- O ideal é que as permissões de acesso deste usuário estejam restritamente limitadas às funções que irá realizar, ou seja, para a exibição de um relatório, a conexão com o banco de dados deve ser realizada por um usuário com permissões de leitura e acesso somente às tabelas necessárias para sua operação

Mecanismos de Controle de

Acesso
planejamen/o e
segurança...

Mecanismos de Controle de

Acesso Definição

O Os mecanismos de controle de acesso são usados para implementar as políticas de autorização.

Define quem pode fazer o que em um sistema.

Se refere a sistemas grandes (S.O., Bancos de Dados, Prontuários de pacientes, etc); **Exemplo mais clássico é o “Esqueci a senha” de um provedor de E-mail.**

Segurança contra

Falhas
planejamen/o e
segurança...

Segurança contra Falhas

Recover

y A recuperação/tolerância a falhas tem por **objetivo restaurar o Banco de Dados para um estado de integridade, após a ocorrência de uma falha.**

Os mecanismos de recuperação baseiam-se na utilização de formas de redundância que quase duplicam o Banco de Dados , utilizando Backup e Log

Segurança contra Falhas

Backup

S Os backups são **cópias de segurança do Banco de Dados**, que são executados periodicamente e constituem um ponto de partida para a recuperação do Banco de Dados após a ocorrência de uma falha, independentemente da sua gravidade.

Segurança contra Falhas

Log

S Os transaction logs são **mecanismos de repetição das transações ocorridas desde o último backup** (rollforward). Normalmente para se refazer uma transação é necessário o ficheiro de transaction log, onde está guardada uma identificação da transação e uma cópia dos dados atualizados por ela (after image).

Tipos de Falhas

*planejamen/o e
segurança...*

Tipos de Falhas

Falha de Disco

O(s) disco(s) armazenado(s) onde o Banco de Dados está É a falha gravee que obriga à reconstrução de todo o SGBD considerada).

Tipos de Falhas

Falha de Sistema

A falha de sistema pode resultar de problemas de hardware ou software, não sendo possível garantir a validade dos dados. Implica repor a Banco de Dados a partir do seu último estado de integridade.

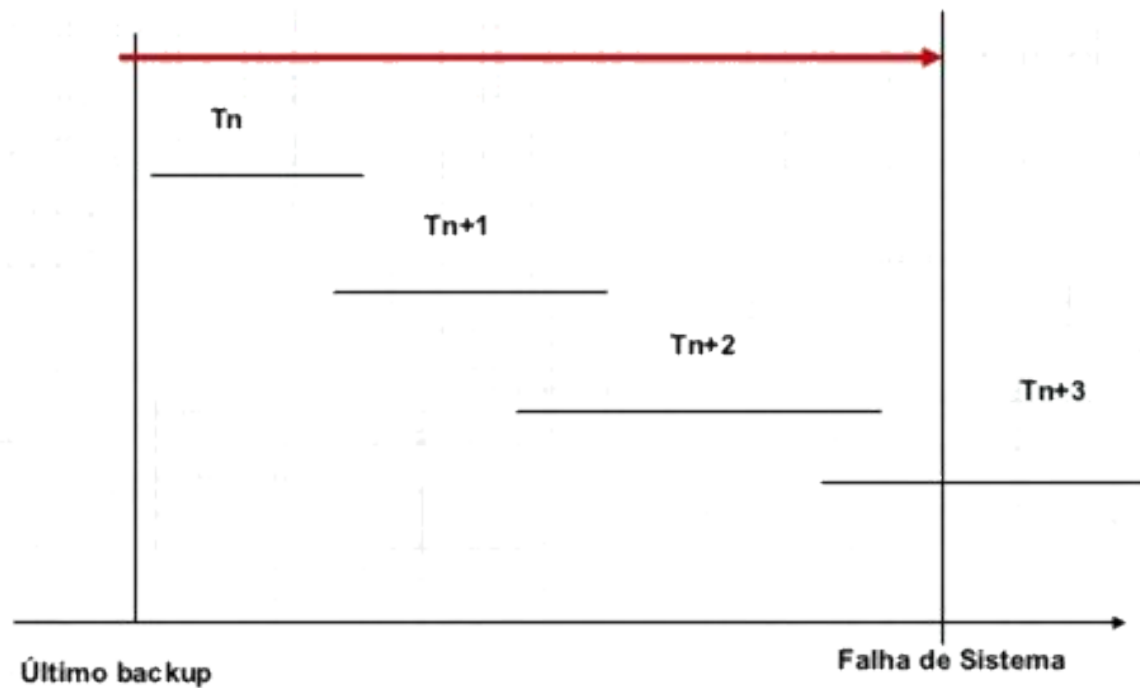
Tipos de Falhas

Falha de Transação

Falha de Transação **é a mais inofensiva e recupera-se recorrendo ao ficheiro transaction log** e às before images da transação que não foi bem sucedida. Em qualquer processo de recuperação recorre-se ao rollback das transações efetuadas até ao momento em que os transaction log e os ficheiros da base estão sincronizados, para se poderem desfazer todas as transações decorridas desde então.

Tipos de Falhas

Falha de Transação



Segurança em

BDs

planejamen/o e

Segurança em

BDs

BD Livre

(MySQL)

- O MySQL sem dúvida nenhuma, é o banco de dados open source mais conhecido do mercado e provavelmente o mais utilizado. Ele é rápido, simples, funcional e hoje implementa recursos que o colocam próximo a grandes nomes como Oracle.
- Apesar de implementar um sistema de validação robusto, o MySQL não tem como controlar acessos que deveriam ser bloqueados pelo sistema operacional. Acesso a arquivos, permissões de usuários do sistema, ou mesmo do usuário sob o qual roda o servidor devem ser especialmente preparados para evitar que haja corrupção ou quebra da privacidade dos dados. Resumindo, apenas o banco de dados MySQL deve ter acesso à aos arquivos de dados do MySQL.

Segurança em

BDs

BD Proprietário

(Oracle)

- A segurança do banco de dados pode ser classificada em duas categorias distintas: segurança de sistema e segurança de dados. A segurança de sistema contém os mecanismos que controlam o acesso e o uso do banco de dados em um determinado nível do sistema. Os mecanismos de segurança do sistema verificam se um usuário está autorizado a se conectar ao banco de dados, se a auditoria do banco de dados está ativa e quais operações de sistemas um usuário pode executar. A segurança de sistema inclui combinações válidas de nome de usuários e senha, a quantidade de espaço em disco disponível para os objetos de esquema de um usuário e os limites de recurso de um usuário.

Segurança em

BDs

BD Proprietário

(Oracle)

- A segurança de dados inclui os mecanismos que controlam o acesso e o uso do banco de dados no nível de objeto de esquema incluindo quais usuários têm acesso a um objeto e a tipos específicos de ações que cada um pode executar. Existem ferramentas adicionais que incrementam a segurança do Oracle Server, possibilitando um ambiente multi plataforma de maior escala. Entre elas podemos citar : Oracle Enterprise Manager (conhecido como OEM) Oracle Security Server Manager (conhecido como OSS).

Linguagen

diferenç
S
as

Linguagens

s

Tipos de Linguagens

- Linguagem de **Marcação**

ex.: HTML, XML;

- Linguagem de **Formatação**

ex.: CSS;

- Linguagem de **Script**

ex.: JavaScript, ActionScript;

- Linguagem de **Programação**

ex.: ASPX, JSP, PHP, Object Pascal, C#;

- Linguagem de **Manipulação de Dados**

ex.: SQL

Front End

Back End

**Banco de
Dados**

Linguagens

Gerenciamento



C R U D
R E P
E E A D
L A D A
E T T
T
F F F

Subconjuntos do

SQL

linguagens

Subconjuntos do SQL

DDL - Linguagem de Definição de Dados

DDL (*Data Definition Language*) são usadas para definir a estrutura de banco de dados ou esquema.

Os comandos básicos DDL são:

- **CREATE**
cria objetos no banco de dados
- **ALTER**
altera a estrutura da base de dados
- **TRUNCATE**
remover todos os registros de uma tabela
- **COMMENT**
adiciona comentários ao dicionário de dados
- **RENAME**
comando para renomear um objeto
- **DROP**
deleta um objeto

Subconjuntos do SQL

DML - Linguagem de Manipulação de Dados

DML (*Data Manipulation Language*) são utilizados para o gerenciamento de dados dentro de objetos do banco.

Os comandos básicos DML são:

- **INSERT**
inserir dados em um banco de dados
- **UPDATE**
atualiza os dados existentes em uma tabela
- **DELETE**
exclui registros de uma tabela

Subconjuntos do SQL

DQL - Linguagem de Consulta de Dados

DQL (*Data Query Language*) é utilizado para a realização de consultas no banco de dados.

O único comando do DQL é:

- **SELECT**

apresenta dados de um banco de dados

Subconjuntos do SQL

DCL - Linguagem de Controle de Dados

DCL (*Data Control Language*) controla os aspectos de autorização de dados e licenças de usuários para controlar quem tem acesso para ver ou manipular dados dentro do banco de dados.

Os comandos básicos DCL são:

- **GRANT**

autoriza ao usuário executar ou setar operações

- **REVOKE**

remove ou restringe a capacidade de um usuário de executar operações

Subconjuntos do SQL

DCL - Linguagem de Controle de Dados

DCL (*Data Control Language*) controla os aspectos de autorização de dados e licenças de usuários para controlar quem tem acesso para ver ou manipular dados dentro do banco de dados.

Os comandos básicos DCL são:

- **GRANT**

autoriza ao usuário executar ou setar operações

- **REVOKE**

remove ou restringe a capacidade de um usuário de executar operações

Subconjuntos do SQL

DTL - Linguagem de Transação de Dados

DTL (*Data Transaction Language*) ou TCL (*Transaction Control Language*) são usados para gerenciar as mudanças feitas por instruções DML . Ele permite que as declarações a serem agrupadas em transações lógicas .

Os comandos básicos DML são:

- **BEGIN WORK**

usado para marcar o começo de uma transação de BD que pode ser completada ou não.

- **COMMIT**

finaliza uma transação dentro de um sistema de gerenciamento de banco de dados.

- **SAVEPOINT**

identificar um ponto em uma transação para que mais tarde você pode efetuar um ROLLBACK

- **ROLLBACK**

faz com que as mudanças nos dados existentes desde o último COMMIT ou ROLLBACK sejam descartadas.

< FIM

*bpra pra
>
casa!*