Banco de Dados

Prof. Carlos Storck

Segurança e Recuperação

- ✓A segurança do banco de dados herda as mesmas dificuldades que a segurança da informação enfrenta, que é garantir a integridade, a disponibilidade e a confidencialidade
- ✓Um sistema gerenciador de banco de dados deve fornecer mecanismos que auxiliem nesta tarefa
- ✓Os bancos de dados SQL implementam mecanismos que restringem ou permitem acessos aos dados de acordo com papeis ou roles fornecidos pelo administrador

Segurança e Recuperação

Tipos de ameaças

- Perda de integridade: modificação inadequada de dados, sabotagem, fraude, atos acidentais
- Indisponibilidade: risco de impedir o acesso legítimo
- Perda de confidencialidade: exposição de dados sensíveis (pessoais, governamentais, corporativos, etc.) a pessoas não autorizadas

Segurança e Recuperação

- ✓Confidencialidade:
  - Garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso
- ✓Integridade:
  - A informação é alterada somente pelas pessoas autorizadas
- ✓Disponibilidade:
  - Garantia de que as pessoas autorizadas obtenham acesso à informação e aos ativos correspondentes sempre que necessário
- ✓Dessa forma, garantir a segurança da informação é fazer com que as informações permaneçam confidenciais, íntegras e disponíveis para a pessoa certa na hora certa

Segurança e Recuperação

✓Um SGBD multiusuário deve fornecer técnicas que possibilitem que certos usuários ou grupos de usuários acessem partes selecionadas de um banco de dados sem obter acesso ao restante do banco de dados

✓Deve evitar que pessoas desautorizadas acessem o próprio sistema – para obter informações ou para realizar alterações maliciosas em uma parte do banco de dados

✓Fornecer proteção para dados especiais – como números de cartões de crédito – que estão sendo transmitidos através de algum tipo de rede de comunicação

Segurança e Recuperação

✓O administrador do banco de dados (DBA) é a autoridade central para gerenciar um sistema de banco de dados

✓As responsabilidades do DBA incluem conceder privilégios a usuários que precisem utilizar o sistema e classificar usuários e dados de acordo com a política da organização

✓Comandos privilegiados do DBA incluem comandos para conceder e revogar privilégios para contas, usuários individuais ou grupos de usuários, e para realizar os seguintes tipos de ações:

- Criação de conta
- Concessão de privilégios
- Revogar privilégios
- Designar nível de segurança

Segurança e Recuperação

Concessão e revogação de privilégios

- GRANT
  - O owner pode conceder os privilégio que possui a outro(s) usuário(s)
  - Um usuário detentor de um privilégio pode passá-lo adiante se tiver recebido o privilégio com a GRANT OPTION
- REVOKE
  - Quem concede um privilégio pode revogá-lo a qualquer momento

Segurança e Recuperação

- ✓Existem diversas causas para as falhas que um dispositivo mecânico ou elétrico pode sofrer, incluindo falha de disco, falta de energia e erros de software
- ✓Além das falhas de sistema, as transações também podem falhar por vários motivos, como violação de restrições de integridade ou impasses (deadlocks)
- ✓No caso de falha, o estado do sistema de banco de dados pode não estar mais consistente, ou seja, ele pode não refletir um estado do mundo que o banco de dados deveria capturar
- ✓Para preservar a consistência, é exigido que cada transação seja atômica
- ✓É responsabilidade do esquema de recuperação garantir as propriedades de atomicidade e durabilidade

Segurança e Recuperação

- ✓Nos esquemas baseados em log, todas as atualizações são registradas em um log, que precisa ser mantido no armazenamento estável (via discos espelhados ou RAID)
- ✓Uma transação é considerada como tendo sido confirmada quando seu último registro de log, que é o registro de log de confirmação para a transação, foi enviado para o armazenamento estável
- ✓Os registros de log contêm valores antigos e novos para todos os itens de dados atualizados
- ✓Os valores novos são usados caso as atualizações precisem ser refeitas após uma falha do sistema
- ✓Os valores antigos são usados para reverter as atualizações da transação caso o sistema tenha falhado antes que a transação fosse confirmada

Segurança e Recuperação

- ✓No esquema de modificações adiadas, durante a execução de uma transação, todas as operações de escrita são adiadas até que a transação tenha sido confirmada, no momento em que o sistema usa a informação no log associado à transação na execução das escritas adiadas
- ✓Com a modificação adiada, os registros de log não precisam conter valores antigos de itens de dados atualizados
- ✓Para reduzir o overhead de pesquisar o log e refazer as transações, podemos usar técnicas de ponto de verificação (checkpoint)
- ✓Algoritmos de recuperação modernos são baseados no conceito de repetição de história, pelo qual todas as ações tomadas durante a operação normal (desde o último ponto de verificação completado) são reproduzidas durante a passada de redo da recuperação

Segurança e Recuperação

✓Para a recuperação de falhas que resultam na perda de armazenamento não volátil, temos de fazer o dump do conteúdo inteiro do banco de dados para o armazenamento estável periodicamente – uma vez por dia, por exemplo

✓Se houver uma falha que resulte na perda de blocos físicos do banco de dados, usamos o dump mais recente na restauração do banco de dados para um estado consistente anterior

✓Quando essa restauração tiver sido realizada, usamos o log para trazer o sistema de banco de dados ao estado consistente mais recente