UNIVERSIDADE ESTADUAL DE SANTA CRUZ (UESC)

Criada pela Lei 6.344, de 05.12.1991,
e reorganizada pela Lei 6.898, de 18.08.1995 e
pela Lei 7.176, de 10.09.1997

CET091 – Banco de Dados II

Prof. Dr. Marcelo Ossamu Honda

Departamento de Ciências Exatas e Tecnológicas (DCET)
mohonda(at)nbcgib(.)uesc(.)br

Sistema de Recuperação

Sistema de Recuperação

- Sistema de computador:
  - Sujeito a falhas;
    - Tipos de falhas:
      - Falhas de hardware;
      - Falhas de software;
      - Falhas externas;
        - Falta de energia;
        - Catástrofes;
  - Informações podem ser perdidas;

Sistema de Recuperação

- Sistema de Banco de Dados;
  - Garantir Atomicidade e Durabilidade das transações;
    - Ações preditivas;
  - Esquema de Recuperação;
    - Podem restaurar o banco de dados ao estado que existia antes da falha;
    - Alta disponibilidade;
      - Reduzir o tempo inoperante após uma falha;

Classificação das Falhas

Classificação das Falhas

- Falha simples;
  - Falhas que não resultam em perda de informações;
- Falhas complexa;
  - Falhas que resultam em perda de informações;
- Tipos de Falha:
  - Falha de transação;
    - Erro lógico: a transação para devido a alguma condição interna;
    - Erro do sistema: sistema enta em um estado de impasse;
  - Falha do sistema;
    - Hardware, sistema de banco de dados ou sistema operacional;
  - Falha de disco;
    - Um ou mais blocos do disco perde seu conteúdo;

Classificação das Falhas

- Para determinar como o sistema deverá se recuperar:
  - Identificar o modo de falha;
  - Modo como a falha afetou o conteúdo do banco de dados;
  - Aplicar algoritmos para garantir:
    - Coerência do banco de dados;
    - Atomicidade da transação apesar das falhas;
- Algoritmos de recuperação:
  - Ações tomadas durante o processamento de transação normal;
    - Informações que suficientes para a recuperação da falha;
  - Ações tomadas após a falha;
    - Para recuperar o conteúdo do banco de dados;
      - Estado consistente, atomicidade do banco de dados e durabilidade dos dados;

Estrutura de Armazenamento

Estrutura de Armazenamento

- Meios de armazenamento e seus métodos de acesso;
  - Determinar como garantir as propriedades de atomicidade e durabilidade de uma transação;
- Tipos de armazenamento:
  - Volátil;
    - Memória principal e memória cache;
  - Não volátil;
    - Discos e fitas magnéticas
  - Estável;
    - Diz que, informações **nunca** são perdidas;
      - Tornar a perda de dados extremamente impossível;

Armazenamento Estável

- Para implementar:
  - Replicar informações em diferentes meios não voláteis independentes;
    - Atualizar a informação de uma maneira controlada para garantir que a falha durante a transferência de dados não danifique a informação necessária;
  - Backup remoto;
    - Remoção de cópias de meios não voláteis;
    - Utilização de redes de computadores;

Recuperação e Atomicidade

Recuperação e Atomicidade

- É responsabilidade do esquema de recuperação garantir as propriedades de atomicidade e durabilidade;
  - Em caso de falha, o estado do sistema de banco de dados pode não estar mais consistente;
    - Não refletir um estado do mundo que o banco de dados deveria capturar;
  - Esquemas simplistas não funcionam;
- Para preservar a consistência, é exigido que cada transação seja atômica;
  - Garantir informações que descrevem as modificações feitas no armazenamento estável, sem modificar o próprio banco de dados;
    - Permite gerar todas as modificações feitas por uma transação;
- Idempotente;
  - Operação redo, mesmo se executada várias vezes, para uma determinada transação precisa ser equivalente à execução de uma única vez;

Recuperação Baseada em LOG

Recuperação Baseada em LOG

- Estrutura mais utilizada para registrar as modificações do banco de dados;
- LOG:
  - É uma sequencia de registros de log;
  - Registrando todas as atividades e atualização no banco de dados;
  - Um registro de log de atualização, deve ter os campos:
    - Identificador da transação;
    - Identificador do item de dados;
    - Valor antigo;
    - Valor novo;
    - Chamado de registros de log físico;
  - Registro de log especiais;
    - Existem para registrar eventos significativos;

$< t_i \text{ start} >$

$< t_i, X_i, V_1, V_2 >$

$< t_i \text{ commit} >$

$< t_i \text{ abort} >$

Recuperação Baseada em LOG

- Sempre que uma transação realiza uma escrita, é essencial que o registro de log para essa escrita seja criado;
  - Antes que o banco de dados seja modificado;
- O registro de log precisa ser utilizar um armazenamento estável;
- O armazenamento do log pode gerar um volume muito grande;

Recuperação Baseada em LOG

- Modificação de Banco de Dados Adiada;
  - Durante a execução de uma transação:
    - Todas as operações write são adiadas;
    - Até que a transação execute um commit parcial;
  - Utilizado as informações no log associado a transação na execução das escritas adiadas;
- Modificação Imediata do Banco de Dados;
  - O sistema aplica todas as atualizações diretamente ao banco de dados;
  - Em caso de falha, o sistema usa a informação do log na restauração do estado do sistema a um estado consistente anterior;

Pontos de Verificação (check points)

- Reduzir a sobrecarga da pesquisa de transações de log e da replicação;
  - Processo de busca demorado;
  - A maioria das transações já enviaram suas atualizações ao banco de dados;
- Constituído pela seguintes ações:
  - Enviar para o armazenamento estável todos os registros atualmente residindo na memória principal;
  - Enviar para o disco todos os blocos de buffer modificados;
  - Enviar para o armazenamento estável um registro de log <checkpoint>;
- Bloqueia todas as transações correntes;
- Melhore os procedimentos de recuperação;

Recuperação com Transações Concorrentes

Recuperação com Transações Concorrentes

- Independentemente do número de transações simultâneas;
  - O sistema tem um único buffer de disco e um único LOG;
  - Todas as transações compartilham bloco de buffer;
  - É permitido a modificação imediata;
  - É permitido que um bloco de buffer tenha itens de dados atualizados por uma ou mais transações;

Recuperação com Transações Concorrentes

- Iteração com o controle de concorrência:
  - O esquema de recuperação depende muito do esquema de controle de concorrência usado;
  - Para reverter uma transação que falhou:
    - Deve ser revertida as atualizações realizadas pela transação;
    - Usando log;
      - É revertido o valor usando a informação de undo em um registro e log;

Recuperação com Transações Concorrentes

- Rollback da transação:
  - É utilizado a varredura do log ao contrário;
    - Uma transação pode ter atualizado um item de dados mais de uma vez;
- Pontos de Verificação:
  - Acrescentando uma lista no registro de log do ponto de verificação;
    - Uma lista (L) de transações ativas no momento do ponto de verificação;
    - <checkpoint L>

Recuperação na Partida

- Recuperação de falha no inicio do sistema de banco de dados;
- Utiliza duas listas:
  - Utiliza o log de trás para frente;
    - Até encontrar o primeiro <checkpoint L>;
  - Lista de undo:
    - Transações a serem desfeitas;
    - Transações que possuem <T start> e não estão na lista redo;
    - Transações que estão na lista do <checkpoint L> e não estão na lista redo;
  - Lista de redo:
    - Transações a sere refeitas;
    - Transações finalizadas com commit;

Falha com Perda de Armazenamento Não Volátil

Falha com Perda de Armazenamento Não Volátil

- Necessário o dump do conteúdo inteiro do banco de dados;
  - Backup que deve ser realizado periodicamente;
  - Contem o conteúdo inteiro do banco de dados;
- Em caso de falha:
  - Primeiro é utilizado o dump mais recente;
    - Para restaurar o banco de dados até um estado consistente anterior;
  - Posteriormente é utilizado o LOG;
    - Para sincronizar o sistema de banco de dados ao estado consistente mais recente;

Plano de Contingência

Plano de Contingência

- Também conhecido:
  - Planejamento de riscos;
  - Plano de continuidade de negócios;
  - Plano de recuperação de desastres;
- Objetivo:
  - Descrever as possíveis causas;
    - Descrição dos cenários;
  - Descrever as medidas a serem tomadas;
    - Ativação de processos manuais;
      - Garantir o funcionamento básico do negócio;
      - Evitar problemas maiores (problemas dos problemas);
- Custo deve ser capitalizado já na fase de projeto;

Plano de Contingência

- Regras para elaborar um Plano de Contingência:
  - Identificar todos os processos de negócio da organização;
    - Para cada processo identificado, avaliar o impacto que a sua falha representa para a organização;
      - Maneira como os processos se interligam;
    - Assim será possível identificar todos processos críticos para a sobrevivência da organização;
  - Identificar riscos e definir cenários possíveis de falha para cada um dos processos críticos;
    - Probabilidade de ocorrência de cada falha;
    - Duração dos efeitos;
    - Consequências resultantes;
    - Custos;
      - Inerentes;
      - Incorridos (quando não existe a contingência);
    - Limites máximos até a ativação da respectiva medida de contingência;
      - Critérios de ativação do plano;
      - Responsável pela ativação do plano;

Plano de Contingência

- Regras para elaborar um Plano de Contingência:
  - Listar as medidas a serem postas em prática caso a falha aconteça;
    - Responsável (e seus suplentes) por colocar em prática as medidas de contingência definidas;
      - Conhecimento do plano;
        - Responsável por decisões adversas e seus limites;
      - Incluindo até o assessor de imprensa;
  - Definir ações necessárias para operacionalização das medidas;
    - Aquisição de novos recursos físicos e/ou humanos;
  - Definir forma de monitoramento após a falha;
  - Definir a forma de como sair do estado de contingência e retornar ao seu estado normal de operação;
    - Definir os responsáveis por estas ações;
    - Definir o monitoramento desse processo;
  - Ações continuadas após operação de um plano de contingência;

Plano de Contingência

- Exemplos:
  - Plano de contingência do consorcio nacional;
    - Testado anualmente (ou conforme contrato atual);
      - Pode ser iniciado pelo próprio consorcio, pela matriz mundial e também pela empresa terceirizada de suporte;
  - Plano de contingência utilizado;
    - Tragédia do Voo da Gol 1907;
      - Outubro de 2006;

Sistemas de Backup Remoto

Sistema de Backup Remoto

- Busca oferecer alta taxa de disponibilidade;
  - Processamento realizado em um site primário;
  - Dados replicados em um site de backup remoto;
    - Site secundário;
    - Deve ser sincronizado com o site primário;
      - Pode utilizar sincronização assíncrona;
      - Pode assumir como site primário;
        - Necessário uma recuperação;
  - Projeto de um sistema de backup remoto deve considerar:
    - Detecção de falha;
    - Transferência de controle;
    - Tempo de recuperação;
    - Tempo para confirmar;
  - Sistemas podem ser:
    - Paralelos ou distribuídos;

Teste do Backup

Teste do Backup

- Proceder ensaios periódicos;
  - Verificar processos e documentação;
  - Toda a equipe deve participar ou ter conhecimento;
    - Hierarquia;
- Considerados por alguns a parte mais importante do processo de backup;
  - Principalmente por ser esquecido;

Backup no PostgreSQL

Chapter 24. Backup and Restore

As with everything that contains valuable data, PostgreSQL databases should be backed up regularly. While the procedure is essentially simple, it is important to have a clear understanding of the underlying techniques and assumptions.

There are three fundamentally different approaches to backing up PostgreSQL data:

- SQL dump
- File system level backup
- Continuous archiving

Each has its own strengths and weaknesses. Each is discussed in turn below.

Referências

- Ramez Elmasri e Shamkant B, Navathe, Sistemas de Banco de Dados, Pearson Addison Wesley, 2005;
- Abraham Silverschatz, Henry F. Korth e S. Sudarshan, Sistema de Banco de Dados, Editora Campus, 2006;
- PostgreSQL 8.3.6 Documentation, by The PostgreSQL Global Development Group, Copyright © 1996-2008 The PostgreSQL Global Development Group;
- http://pt.wikipedia.org/wiki/Plano_de_Conting%C3%AAncia