

ALUNO: Jean William da Costa Buzaglo - 2255693

Estudo de Caso 1 - Falha no Sistema de Pagamento Distribuído

Contexto:

Uma empresa de e-commerce utiliza um sistema distribuído para processar pagamentos. O sistema é composto por três servidores:

- **Servidor A:** Recebe as requisições de pagamento.
- **Servidor B:** Processa as transações e verifica saldo.
- **Servidor C:** Confirma e registra as transações no banco de dados central.

Durante um grande evento promocional, o **Servidor B** apresentou uma **falha intermitente**, fazendo com que algumas transações ficassem em estado indefinido — o cliente foi cobrado, mas a compra não apareceu como confirmada.

Tarefas :

1. Explique **quais tipos de falhas** podem ter ocorrido nesse cenário (falha de processo, de comunicação, bizantina etc.).

Pode ter ocorrido falha de processo no Servidor B (como travamento ou reinício durante o processamento), falha de comunicação com mensagens perdidas, atrasadas ou duplicadas entre os servidores e, em casos mais raros, falha bizantina, quando o servidor passa a enviar respostas incoerentes ou inconsistentes.

2. Indique **como o sistema poderia implementar tolerância a falhas** para evitar a perda ou duplicação de transações.

Para tolerar falhas, o sistema poderia usar replicação do Servidor B para garantir continuidade, registrar cada etapa da transação para permitir reexecução sem duplicações e trabalhar com mensagens idempotentes, evitando cobrança em dobro caso o processamento precise ser repetido.

3. Sugira **uma técnica de recuperação** adequada (ex.: *checkpoint*, *rollback recovery*, *replicação*).

Uma técnica de recuperação adequada seria o uso de *checkpoint* com *rollback*, salvando estados periódicos e retornando ao último estado consistente em caso de falha. Também pode ser usada replicação de estado se quiser reduzir interrupções.

4. Descreva como o **protocolo de comprometimento distribuído (2PC)** poderia ser aplicado para garantir a atomicidade das transações.

No protocolo 2PC, primeiro acontece a fase "prepare", em que B e C informam

se estão prontos para finalizar a transação. Em seguida vem o "commit", que só é executado se todos confirmarem. Isso garante que a transação ou completa totalmente ou é cancelada, mantendo a atomicidade.

5. Aponte uma **medida de segurança** que deveria ser adotada para garantir a integridade dos dados trafegados entre os servidores.

Uma medida de segurança importante é usar criptografia de ponta a ponta, como TLS, para proteger os dados que trafegam entre os servidores e evitar interceptações ou alterações.

Estudo de Caso 2 - Falha de Comunicação e Segurança em Sistema de Monitoramento

Contexto:

Uma empresa de energia elétrica utiliza um **sistema distribuído de monitoramento** de subestações. Cada unidade envia periodicamente dados de tensão e corrente a um servidor central.

Durante uma tempestade, houve instabilidade na rede e perda de pacotes. Além disso, foi detectada a **interceptação de dados** por um agente externo (ataque *man-in-the-middle*).

Tarefas:

1. Classifique as **falhas ocorridas** (falha de comunicação, omissão, segurança etc.).

As falhas envolvem falha de comunicação devido à instabilidade da rede, falha por omissão pela perda de pacotes e falha de segurança por causa do ataque *man-in-the-middle* que interceptou os dados.

2. Explique como a **comunicação confiável** poderia minimizar a perda de pacotes.

A comunicação confiável poderia minimizar perdas usando confirmações de recebimento, retransmissão automática de pacotes não confirmados e controle de timeout para evitar que dados simplesmente se percam no caminho.

3. Descreva uma **estratégia de resiliência** que permita manter o funcionamento parcial do sistema mesmo com perda de conectividade.

Uma estratégia de resiliência seria manter buffers locais nas subestações para armazenar dados temporariamente e operar em modo degradado, enviando tudo quando a conexão voltar, garantindo que o sistema continue funcionando mesmo parcialmente.

4. Aponte **mecanismos de segurança** que devem ser implementados para proteger os dados durante a transmissão.

Os mecanismos de segurança recomendados incluem criptografia forte (como TLS), autenticação entre os dispositivos, verificação de integridade das mensagens e uso de certificados digitais para evitar interceptações.

5. Proponha uma **política de recuperação** após o restabelecimento da rede.

Após o restabelecimento da rede, a política de recuperação pode incluir reenviar os dados armazenados nos buffers, sincronizar o relógio e o estado com o servidor central e validar possíveis inconsistências geradas durante o período offline.
