Trabalho de Segurança e Auditoria de Sistemas - Análise em Arquivos de Log de Sistemas Gerenciadores de Banco de Dados

Discente: Gustavo Santos Teixeira
Matrícula: 202200149

10 de julho de 2025

Com base na análise do arquivo de log proveniente do sistema gerenciador de banco de dados *MySQL*, foram identificadas diversas ações relevantes que permitem a caracterização das transações realizadas, o controle de acesso ao sistema, além da identificação de possíveis pontos de controle e auditoria.

O arquivo inicia com o registro da inicialização do serviço do *MySQL Server*, evidenciado pela linha de execução do processo "mysqld.exe". Em seguida, observa-se a tentativa de acesso por parte do usuário "root@localhost", utilizando conexão segura via SSL/TLS, associada ao thread ID 11. Essa tentativa é sucedida por comandos de configuração de sessão, como *set autocommit*=1, *SELECT current_user*(), *show character set*, *SET NAMES, SHOW VARIABLES* e *SHOW GLOBAL STATUS*, indicando que o acesso foi concedido e que se tratava de uma conexão administrativa para verificar parâmetros do ambiente. Outra conexão similar, utilizando o *thread* ID 12, é registrada na mesma sequência de tempo, reforçando a hipótese de múltiplas sessões simultâneas de administração.

Posteriormente, com o *thread* ID 10, são iniciadas diversas ações transacionais no banco de dados. A sequência inicia-se com a criação do esquema denominado universidade, seguido por comandos de seleção de banco e por consultas para verificar o estado atual do sistema (*SELECT DATABASE()*). Na sequência, são executadas instruções de manipulação de estrutura de dados, como *DROP TABLE IF EXISTS e CREATE TABLE,* evidenciando a intenção de reconstruir a base de dados. Tais ações compreendem a exclusão e recriação das tabelas pessoa, aluno, colaborador, livro e emprestimo, todas estruturadas com chave primária e restrições de integridade referencial através de chaves estrangeiras, o que demonstra uma atenção à normalização e à consistência dos dados.

É possível afirmar que essas transações foram efetivadas, dado que não há registros de erro ou mensagens de falha entre os comandos. Todas as operações seguem uma sequência lógica e completa de execução, com uso de comandos *SHOW WARNINGS*, que indicam boas práticas de verificação após operações sensíveis como *DROP TABLE.*

Quanto aos pontos de controle, pode-se considerar o uso explícito do comando *SET autocommit*=1 como um mecanismo de controle transacional automático, onde cada operação é tratada como uma transação individual imediatamente efetivada. Ainda que não haja uso explícito de *BEGIN, COMMIT ou ROLLBACK*, o controle automático por transação implícita já representa um ponto de controle no ambiente. A ausência de comandos de reversão de transações ou de erros indica que não foram detectadas transações canceladas ou falhas no processo analisado.

Sob o ponto de vista de auditoria, o *log* apresenta registros suficientes para reconstruir parte das atividades administrativas realizadas no SGBD, especialmente as relacionadas à definição da estrutura do banco. Contudo, a ausência de informações como alteração ou inserção de dados (operações *INSERT, UPDATE, DELETE*) limita a abrangência da auditoria apenas à fase de modelagem e estruturação do sistema. Destaca-se ainda que a repetição do uso da conta *root* para todas as ações representa um possível ponto de auditoria crítico, uma vez que boas práticas de segurança recomendam a segregação de privilégios e o uso de usuários distintos para diferentes tipos de operação.

Como recomendações, sugere-se:

- A criação de usuários específicos com privilégios limitados para operações distintas, evitando o uso contínuo da conta *root*;
- A implementação de *logs* mais detalhados, com registros de alterações em dados, para permitir uma auditoria mais completa;
- A verificação periódica de integridade referencial, dado o uso extensivo de chaves estrangeiras;

- A definição de políticas de controle transacional mais explícitas, com uso de *BEGIN, COMMIT e ROLLBACK*, permitindo maior rastreabilidade das transações.

Portanto, a análise dos logs evidencia uma sequência de transações estruturais efetivadas com sucesso, acessos ao sistema realizados com segurança via SSL, e pontos de controle baseados no uso de autocommit. A centralização de ações na conta root representa um ponto de auditoria que pode comprometer a rastreabilidade e a segurança, sendo necessário adotar alternativas para garantir melhores práticas de controle interno.