REVISTA DE CIÊNCIAS EXATAS E TECNOLOGIA

AUDITORIA EM BANCO DE DADOS COM UTILIZAÇÃO DE REGRAS

Eder Pazinatto – *Faculdade Anhanguera de Passo Fundo*

RESUMO: A busca por mecanismos que implementam segurança nos sistemas e aplicações que envolvem banco de dados é cada vez maior. Um das formas de prover essa segurança e controle dos dados é através da auditoria de banco de dados. Os Sistemas Gerenciadores de Banco de Dados(SGBDs) possuem recursos para a implementação de técnicas de auditoria. O PostgreSQL implementa rules (regras) que possibilitam auditar o banco de dados registrando alterações (ou tentativas) feitas nos dados, informação de quem o alterou e quando este dado foi alterado. No PostgreSQL uma regra de auditoria sobre uma tabela é facilmente criada através de comandos SQL(Structured Query Language). Depois de criada, a regra passa a auditar de forma automática (sem intervenção humana) as operações realizadas sobre os dados. As rules do PostgreSQL representam um recurso simples e eficiente que os administradores de banco de dados podem utilizar para fazer auditaria em banco de dados.

PALAVRAS-CHAVE:
banco de dados; auditoria; regras; segurança

ABSTRACT: The search for mechanisms that implement security in the systems and applications that involve database is every time more important. One of the ways of providing that security and control of the data is through the database audit. The Database Management System (DBMS) has resources for the implementation of audit techniques. PostgreSQL implements rules that make it possible to audit the database registering changes (or tries) done in the data, information about who changed it and when it was changed. In PostgreSQL an audit rule on a table is easily created through commands SQL(Structured Query Language). After being created, the rule starts auditing the operations accomplished on the data in an automatic way (without human intervention). The rules of PostgreSQL represent a simple and efficient resource that the database administrators can use to audit database

KEYWORDS:
database; audit; rules; security

Artigo Original
Recebido em:23/10/2009
Avaliado em: 14/12/2010
Publicado em: 22/04/2014

Publicação
Anhanguera Educacional Ltda.

Coordenação
Instituto de Pesquisas Aplicadas e Desenvolvimento Educacional - IPADE

Correspondência
rc.ipade@anhanguera.com

1. INTRODUÇÃO

Atualmente nas empresas a informação torna-se cada vez mais importante, e o volume de dados que geram a informação aumentam de forma exponencial a cada ano. No processo de gestão e gerenciamento de informações, várias tecnologias são usadas com adoção de banco de dados.

O uso das informações, facilitado pelo avanço da Tecnologia de Informação e Comunicação (TIC), passa a ter papel fundamental nas organizações, possibilitando melhor percepção das mudanças, maior flexibilidade e agilidade nas operações (FERREIRA; ASSUMPÇÃO, 2005). No gerenciamento dessas informações com a TIC, vários elementos são envolvidos na estrutura dos dados.

A utilização de banco de dados é fundamental para que o processo de geração de informações seja mantido de forma íntegra. O armazenamento e a recuperação de informações precisam ser feitas de forma ágil e eficiente (LAUDON; LAUDON, 2007). Nesse processo, a gestão dos dados e a segurança da informação devem ser vistos como componentes de um sistema mais amplo que objetiva suportar o crescimento organizado das empresas, a definição de estratégia e o fomento da governança corporativa.

A informação é um ativo muito valioso para as empresas, sujeita a um volume enorme de ameaças que pode colocar em risco a continuidade do negócio (OLIVEIRA, 2006). Portanto, as empresas estão cada vez mais sujeitas a agentes que podem provocar vazamento de conhecimento, indisponibilidade de serviços, de documentos ou informação relevante.

As empresas enfrentam um mercado altamente competitivo, globalizado e turbulento (FRANCO, 2009). Essa situação pode gerar necessidades de adequação e ajustes dentro de suas operações e processos do cotidiano, levando em consideração carências dos processos internos e/ou externas em que estão inseridas. Nesse sentido, as organizações precisam de segurança nos dados, para que informações e conhecimentos possam auxiliar com segurança os processos decisórios e sua gestão.

No processo de organização, gerenciamento e segurança de dados para o processo de gestão, existem várias tecnologias e ferramentas de banco de dados que podem executar esse papel. Contudo, essas tecnologias precisam ser implementadas e bem gerenciadas para que possam fornecer o resultado esperado.

O objetivo desse artigo é apresentar uma abordagem para auditoria da base de dados, representada em forma de tabelas estruturadas no banco de dados. Para isso, é apresentada uma explanação geral sobre as ferramentas e técnicas disponíveis para realização da auditoria de serviços e operações realizadas na base de dados.

2. BANCO DE DADOS

Um banco de dados é uma coleção de dados relacionados (ELMASRI, 2005). Podemos considerar que os dados são fatos que podem ser gravados e possuem um significado para determinado fim (e/ou aplicação). Os dados são armazenados de forma estruturada, facilitando sua organização e posteriormente sua recuperação.

A organização de um banco de dados está conforme seu modelo de dados. Um modelo de dados fornece detalhes de armazenamento dos dados (SILBERSCHATZ; KORTH, 2005). No modelo de dados estão descritos os tipos de dados, relacionamentos e estruturas que devem suportar os dados.

Para implementação, há uma coleção de programas que permitem os usuários criar e manter um banco de dados, esse programas são conhecidos como Sistemas Gerenciadores de Banco de Dados (SGBDs). O SGBD é um sistema de software de propósito geral que facilita os processo de definição, construção, manipulação e compartilhamento de banco de dados entre vários usuários e aplicações (ELMASRI, 2005).

Os Sistemas Gerenciadores de Banco de Dados proporcionam uma camada de software para trabalhar diretamente com os dados no banco de dados. Essa camada facilita o gerenciamento, definição das funcionalidades e criação de usuários com diferentes permissões de acesso e modificação de dados. Esses diferentes níveis de usuários proporcionam segurança e facilitam o gerenciamento e auditoria sobre a base de dados. Dentre esses usuários destaca-se a figura do Administrador do Banco de Dados(DBA), usuário que possui todas as permissões de acesso ao banco de dados.

A segurança em banco de dados é uma área bastante ampla que se refere a muitas questões (ELMASRI, 2005). Essas questões podem ser: legais ou éticas referentes ao acesso a certas informações; questões políticas com a definição de quais informações não podem ser tornadas públicas; e questões relacionadas a sistemas, com definição de quais níveis do sistema as funções de segurança devem ser implementadas. O DBA é o responsável pela segurança geral do sistema de banco de dados. Ações como criação de usuários/contas, concessão de privilégios e atribuição de níveis de segurança são de responsabilidade direta do DBA.Conforme a metodologia aplicada, têm-se modelos diferentes para definir a estrutura do modelo de dados. Entre esses modelos, encontram-se o relacional, em rede, hierárquico, Objeto-Relacional e orientado a objetos (SILBERSCHATZ; KORTH, 2005). Para cada modelo existem características específicas de modelagem e softwares de Sistemas Gerenciadores de Banco de Dados usados para implementação.

Com pesquisas e descobertas de novas tecnologias as empresas desenvolvedoras ou comunidades que mantêm Sistemas Gerenciadores de Banco de Dados estão avançando com soluções inovadoras e maiores possibilidades no processo de gerenciamentos de banco de dados. Hoje, há várias opções de sistemas de gerenciamento que necessitam de licenças

para uso tais como Oracle, IBM DB2, Microsoft SQL Server ou gratuitas como MySQL ou PostgreSQL.

Independente do sistema gerenciador de banco de dados, todos apresentam várias tecnologias e funções para melhorar gerenciar e auditar os dados e usuários. As soluções livres, como o PostgreSQL, apresentam alternativas suficientes para implementar recursos para a melhor gestão dos dados. Dentre as funções implementadas pelos SGBDs, a auditoria é usada para gerenciamento e controle de operações no banco de dados.

2.1 Auditoria

A auditoria é um processo de exame, sistemático e independente das atividades desenvolvidas com o objetivo de averiguar se elas estão de acordo com as disposições planejadas e/ou estabelecidas previamente (PADOVEZE, 2004). Na computação, especificamente na área de banco de dados, a auditoria está relacionada ao processo de identificação e proteção do banco contra pessoas que não estão autorizadas a acessar determinadas partes ou todo o bando de dados.

A atividade de auditoria do banco de dados é realizada geralmente pelo DBA. Dentre as várias atividades desenvolvidas pelo administrador uma das mais importantes é o diagnóstico de problemas de execução do SGBD e o monitoramente das operações realizadas pelos usuários do banco de dados (MEDEIROS, 2006).

O SGBD deve prover mecanismos que permitam o DBA auditar o banco de dados. Dentre esses mecanismos o DBA deve ter acesso aos comandos que foram executados, com a finalidade de diagnosticar eventuais exclusões e alterações indevidas nos dados. Conforme o nível de segurança, também deve ser possível identificar tentativas de alterações na base de dados.

Uma solução simples de auditoria é a implementação de Logs que gravam as operações realizadas no servidor de banco de dados em arquivos, permitindo posteriormente a visualização de todas as atividades no servidor. O Log é uma seqüência de registros que mantém um arquivo atualizado das atividades no banco de dados (SILBERSCHATZ; KORTH, 2005).

Outra forma para realização de auditoria é através de regras (ELMASRI, 2005). As regras podem ser criadas (ou acionadas) no SGBD e então os registros de auditoria podem ser gravados em uma tabela física no banco de dados, criada especialmente para essa finalidade. Esse tipo de auditoria pode ser usado com comando de manipulação do banco de dados (DML – *Data Manipulation Language, como Insert, Update e Delete*) ou comandos de definição do banco de dados (DDL- *Data Definition Language, como Create, Drop e Alter*). A auditoria com comandos DDL é também conhecida como auditoria de mudanças de estrutura.

As regras são implementadas por vários SGBDs, com algumas especificidades

particulares a cada SGBD. No PostgreSQL há um sistema de regras (rule system) que oferece recursos e a possibilidade de implementar determinadas regras (Rules) de negócio para a aplicação.

3. UTILIZAÇÃO DE RULES PARA AUDITORIA EM BANCO DE DADOS

Atualmente as organizações possuem a necessidade de que todas operações (ou grande parte delas), executadas no banco de dados, sejam auditadas posteriormente. Práticas de auditoria são comuns e muito úteis no processo de segurança, identificação de discrepâncias na base ou no processo de correção de problemas, às vezes gerados por bugs na aplicação.

No PostgreSQL na versão 8.3, as rules assim como os triggers(gatilhos), são chamadas de regras e são acionadas quando um determinado evento ocorrer em uma tabela do banco de dados. Apesar de desempenharem funções semelhantes rules e triggers possuem diferenças fundamentais (GUEDES, 2005). Por exemplo: com a realização de um comando uma rule é executada uma única vez, ao contrário dos triggers que são executados para cada linha afetada pelo comando que o disparou.

O trigger é um recurso de programação presente na maioria dos SGBDs. Ele é utilizado para associar um procedimento a um evento do banco de dados (inclusão, exclusão, atualização, etc..) de modo qu e o procedimento seja executado automaticamente sempre que o evento associado ocorrer (BUENO; SILVA, 2006).

A auditoria de um banco de dados pode ser implementada com a utilização de uma rule, por exemplo, com a regra que registre todas as operações de alterações (ou tentativas) do campo salário da tabela de funcionários de uma empresa. Assim que o usuário do banco de dados tentar atualizar a tabela com o novo valor de salário, uma rule é disparada e todas as informações deste processo são registradas no banco de dados em uma tabela de auditoria, sem que a alteração seja efetivada na tabela de funcionários e de forma oculta ao usuário que realizou a ação de atualização.

Na implementação da auditoria com rules, foi considerada como base uma tabela simples, chamada "Funcionário" (Tabela 1), com a finalidade de armazenar os dados dos funcionários de uma empresa.

Tabela 1 – Estrutura da tabela "Funcionário"

Funcionário	
id_func	integer
nome	varchar(40)
data_adm	date
cargo	varchar(20)
salario	numeric

A implementação do processo de auditoria foi realizada com uso de SGBD PostgreSQL - versão 8.3 e com a ferramenta de administração PgAdmin III versão 1.8.4, conforme apresentado na Figura1.

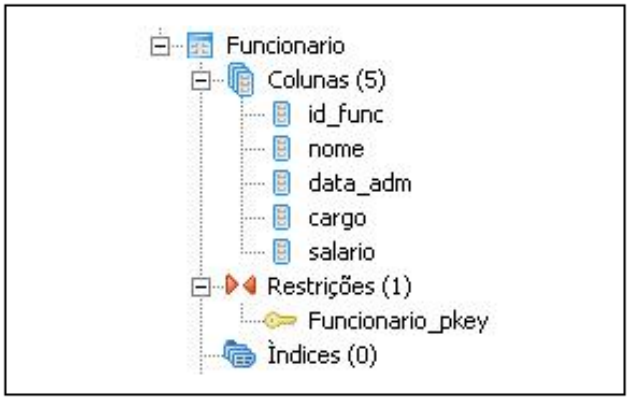

Figura 1 – Tabela "Funcionario" implementada no PostgreSQL

A tabela "Funcionario" possui cinco campos: identificação do funcionário(id_func); nome; data de admissão(data_adm); cargo e salário.

O próximo passo foi criar uma tabela de auditoria – "Func_auditoria" (Tabela 2), que armazena as informações da auditoria de acessos aos dados, alterações ou tentativas de usuários sem permissão. Essa tabela possui os seguintes campos: número de identificação do funcionário, o valor do salário que foi atribuído a esse funcionário, o usuário de banco de dados que fez ou tentou fazer a alteração, a data e a hora que a tentativa de alteração ocorreu.

Tabela 2 – Estrutura da tabela "Func_auditoria"

Func_auditoria	
id_func	integer
novo_salario	numeric
usuario	varchar(30)
datahora	timestamp

Na Figura 2, está representada a tabela "Func_auditoria".

Figura 2 – tabela "Func_auditoria" implementada no PostgreSQL

Depois de criada as duas tabelas, foi necessário criar a rule de auditoria sobre a tabela "Funcionario", para que funcione como uma regra. A rule foi criada através do comando *Create Rule*, sobre a tabela "Funcionario", pois é ela que pode sofrer a tentativa de alteração. Na criação da rule precisa-se seguir a sintaxe do PostgreSQL para utilização de rules:

Nome da Rule: nome da regra;

Evento: indica qual evento(insert, delete, update, select) está associado a regra;

Tabela: tabela a qual a regra está associada;

Condição: uma condição que acione a regra;

Ação: especifica a ação que será executada com o acionamento da regra.

O comando de criação da rule está apresentado na Tabela

Tabela 3- Comando de criação da rule

Linha	Comando
1	CREATE OR REPLACE RULE func_aud_rule AS ON UPDATE TO "Funcionario"
2	WHERE NEW.salario <> OLD.salario
3	DO INSTEAD INSERT INTO "Func_auditoria" VALUES (NEW.id_func,
4	New.salario, current_user, current_timestamp);

A seguir está a explicação do comando de criação da rule (Tabela 3):

Linha 1- cria a rule com o nome "func_aud_rule", sobre a tabela "Funcionario", na ação de atualização desta tabela;

Linha 2- A rule é acionada quando houver uma atualização de salário, desde que o valor informado para o salário seja diferente do valor do salário atual (tabela "Funcionário");

Linhas 3 e 4-Se o valor do salário for diferente, insere as informações (id_func, novo salário, usuário e data e hora) na tabela "Func_auditoria". O comando INSTEAD, faz com que a alteração (novo valor de salário) não seja efetivada/gravada na tabela "Funcionario".

Na recuperação das informações do usuário conectado ao banco de dados, com a data e a hora da tentativa de alteração são usadas respectivamente as funções current_user e current_timestamp, implementadas pelo SGBD PostgreSQL (v. 8.3).

Antes da rule ser acionada, foi abastecida a tabela "Funcionario" com algumas informações, conforme apresentado na Figura 3.

	id_func [PK] integer	nome character(50	data_adm date	cargo character(20	salario numeric
1	1009	Mathias	2006-01-25	Gerente	1520
2	1010	Malaquias	2004-07-05	Analista	779.25
3	1011	Josue	2001-01-04	Auxiliar 1	700.96
4	1012	Tobias	2008-10-14	Desenvolvedor	655.89

Figura 3- Informações armazenadas na tabela "Funcionario

Conforme a definição da rule (tabela 3), a regra é acionada de forma automática no momento que houver uma tentativa de alteração do campo salário da tabela "Funcionario". O script SQL (Structured Query Language) de atualização do quadro 1, demonstra o exemplo de um processo de atualização na tabela funcionário:

Conforme a definição da rule (tabela 3), a regra é acionada de forma automática no momento que houver uma tentativa de alteração do campo salário da tabela "Funcionario". O script SQL (Structured Query Language) de atualização do quadro 1, demonstra o exemplo de um processo de atualização na tabela funcionário:

Quadro 1- Comando de atualização da tabela "Funcionario

```
UPDATE    "Funcionario"
SET       salário = 1010.35
WHERE     id_func = 1011;
```

A execução do script SQL do quadro 1, faz o acionamento automático da rule, pois o salário do funcionário com número de identificação "1011" (da tabela "Funcionario") é diferente do valor do salário atribuído no momento da atualização.

Com o acionamento da regra os dados n_emp, salario, *current_user*(usuário logado no BD), *current_timestamp*(data e hora atual do sistema), serão inseridos na tabela de auditoria, conforme apresentado nos registro 1 da tabela "Func_auditoria" na Figura 4.

	id_func integer	novo_salario numeric	usuario character varying(30)	datahora timestamp withou
1	1011	1010.35	prod_1	2009-08-05 20:35:35
2	1011	1000.84	prod_1	2009-09-03 10:37:06
3	1012	950.89	lobo	2009-09-04 17:40:46

Figura 4- Informações adicionadas na tabela "Func_auditoria"

Conforme apresentando na tabela "Func_auditoria" (usada para fazer a auditoria da tabela "Funcionario") o usuário "prod_1", tentou alterar duas vezes o valor do salário da tabela "Funcionario", em datas diferentes (05-08-2009 e 03-09-2009) e valores de salário diferentes (1010.35 e 1000.84). A tabela de auditoria também registrou que outro usuário - "lobo", também tentou alterar o valor do salário para o valor 950.89. No campo "datahora", estão registradas a data e a hora da tentativa de alteração.

No momento da criação da rule "func_aud_rule" foi definido que comandos de atualização do campo salário não são gravados/efetivados na tabela "Funcionario" e sim, apenas a tentativa de alteração com suas informações (dados), na tabela de auditoria. Na criação de rules podem ser criadas outras definições, depende da finalidade e informações que se deseja auditar.

Para desfazer uma rule ou deixar que a auditoria seja executada é preciso excluir a regra sobre a tabela do banco de dados que ela foi criada. A rule não pode ser desabilitada, apenas excluída com o comando SQL *drop.*

4. CONSIDERAÇÕES FINAIS

Atendendo a busca cada vez maior por segurança na base de dados, soluções com auditoria do banco de dados podem ser feitas de várias formas. A implementação de regras com a utilização de rules do PostgreSQL é uma forma eficiente e simples de auditoria que pode ser facilmente adicionada em qualquer aplicação, pois é executada de forma automática exclusivamente pelo sistema gerenciador de banco de dados com baixo custo de processamento.

As rules podem ser usadas no banco de dados como complemento da utilização de triggers, que são mais conhecidas e por isso, mais usadas. A implementação é feita apenas com comandos SQL, facilitando a implementação e tornando o código de fácil compreensão.

A auditoria com rules pode ser explorada com regras mais completas, condições diferenciadas e ações diferentes na sua execução, conforme a finalidade da auditoria. Há uma série de opções que podem ser adicionadas as rules tornando a regra mais abrangente. Nesse artigo foi usado um exemplo simples, apenas para auditar tentativas de alteração de um campo de uma tabela por usuário não habilitados para esse fim.

O uso da auditoria para registrar tentativas ou alterações na base dados é útil para o aumento da segurança, com o registro automático das alterações realizadas e com informações de quando, como, onde e que alteração ou tentativa de modificação foi realizada. A auditoria também pode ser usada como meio de fornecer um histórico de alterações na base de dados com relação aos dados e a própria estrutura do banco de dados.

REFERÊNCIAS BIBLIOGRÁFICAS

BUENO, Guimarães M. C.; SILVA Corrêa O. da; **Auditoria de sistemas**. SQL Magazine. ed. 38, Rio de Janeiro, 2006

ELMASRI, Navathe. **Sistema de Banco de Dados.** Ed. 4 Pearson, São Paulo, 2005

FERREIRA, K. A.; ASSUMPÇÃO, M.R. **Logística e troca eletrônica de informação em empresas automobilísticas e alimentícias**. Produção (São Paulo), São Paulo, v. 15, n. 3, p. 434-447, 2005.

GUEDES, Bartz G.; **Usando rules no PostgreSQL**. SQL Magazine. ed. 21, Rio de Janeiro, 2005

LAUDON, Kenneth; LAUDON, Jane P.**. Sistemas de Informação Gerenciais**. ed. 7. São Paulo: Prentice Hall Brasil, 2007.

MEDEIROS, M. **Banco de Dados para Sistemas de Informação** Ed. 1, Rio de Janeiro, Visual Books, 2006

OLIVEIRA, de F. Bayma(organizadora). **Tecnologia da Informação e Comunicação: desafios e propostas estratégicas para o desenvolvimento dos negócios**. Fundação Getúlio Vargas, Pearson Prentice Hall:São Paulo, 2006

PADOVEZE, Clovis Luis. **Sistemas de Informações Contábeis: fundamentos e análise.** 4. Ed. São Paulo: Atlas, 2004.

SILBERSCHATZ, A.; KORTH, H., F. **Sistemas de Banco de Dados** Ed.4, Rio de Janeiro LTC, 2005