Auditoria em Banco de Dados: Um estudo sobre a Implementação e Técnicas de Auditoria

Denis F. de Oliveira, Edson C. de Oliveira, Gustavo Bruschi

Curso de Tecnologia em Banco de Dados – Faculdade de Tecnologia de Bauru (FATEC)
Rua Manoel Bento da Cruz nº 30 Quadra 03 – Centro – 17.015-171 – Bauru, SP - Brasil

(denisoliveiraa@hotmail.com, edson.cavalaro@gmail.com, gustavo.bruschi@fatec.sp.gov.br)

Abstract. *With the increase in the volume of data manipulated by the companies, the search for information security is increasing and the audit proposes the control of the instructions made by each user within the Database, monitoring and registering those accesses. The purpose of this work was to present a study on database auditing, showing the importance it has for a company, and proposing an approach using Oracle Audit Vault Software, presenting several features and functionalities and comparing it with a standard audit. It is concluded that for a safe audit and with data integrity, it is necessary to use appropriate Software.*

Resumo. *Com o crescimento do volume de dados manipulados pelas empresas, a busca por segurança da informação é cada vez maior e a auditoria propõe o controle das instruções realizadas por cada usuário dentro do Banco de Dados, monitorando e registrando esses acessos. O propósito deste trabalho foi apresentar um estudo sobre auditoria em banco de dados, mostrando a importância que possui para uma empresa, além de propor uma abordagem utilizando o Software Oracle Audit Vault, apresentando diversos recursos e funcionalidades e o comparando com uma auditoria padrão. Conclui-se que para uma auditoria segura e com dados íntegros, se faz necessário o uso de Softwares apropriados.*

1. Introdução

A segurança da informação, torna-se cada vez mais necessária devido ao alto volume de dados que as empresas manipulam diariamente, aumentando de forma exponencial a cada ano. Para o gerenciamento dessas informações, se faz necessário a utilização de tecnologias como a adoção de um banco de dados.

O banco de dados é fundamental em uma empresa, para garantir que as informações sejam mantidas de forma íntegra, segura e disponível. A gestão dos dados e a segurança devem estar no planejamento como uma das prioridades para suportar o

crescimento organizado, com a definição clara da estratégia para a estimulação da governança corporativa.

Os dados são muito valiosos para tomada de decisões e necessitam de um rigoroso controle de acesso, para não cair em mãos erradas, como concorrentes e pessoas de má índole. A necessidade de se auditar um banco de dados de uma empresa, justifica-se pelo alto valor agregado das informações e a proteção do banco de dados contra pessoas não autorizadas a acessar partes ou todo o banco de dados.

O objetivo proposto foi comparar o processo de auditoria em um banco de dados utilizando o Sistema Gerenciador de Banco de Dados (SGBD) Oracle e a ferramenta Oracle Audit Vault, com uma auditoria padrão utilizando mecanismo automático da Oracle. Com isto, foram realizadas várias instruções, e em seguida, visualizadas através de logs, a fim de analisar e mostrar a importância de uma auditoria no Banco de dados de uma empresa, prevenindo e detectando problemas no cumprimento das regras do negócio.

2. Segurança da Informação

Com a evolução tecnológica que temos a cada dia, as informações que as empresas coletam diariamente vem sendo armazenadas digitalmente, deixando de lado o armazenamento em papel como antigamente. Com essa evolução, busca-se constantemente na segurança da informação, confidencialidade, integridade e disponibilidade desses dados. A segurança da informação de uma empresa, em muitos casos, garante a continuidade do negócio, incrementando estabilidade e permitindo que as pessoas e bens estejam seguros de ameaças cibernéticas. [Bluephoenix 2008]

Com as tecnologias de hoje, podemos prevenir ataques cibernéticos, detectar a origem e recuperar as informações caso seja necessário. Para deixar um ambiente seguro, é necessário analisar as vulnerabilidades de onde as informações são armazenadas, para assim, investir em mecanismos de segurança como prevenção e recuperação.

Os mecanismos de segurança são, medidas que visam monitorar e controlar o acesso às informações de forma física e lógica. Enquanto controles físicos limitam o contato direto as informações que um usuário pode ter, o controle lógico assegura a integridade da informação, de modo que ela não seja acessada nem manipulada por pessoas não autorizadas. Alguns destes mecanismos de segurança são a criptografia de dados, que converte os dados em um formato que seja impossível decodificá-lo, a não ser o próprio software que fez essa criptografia. Outro mecanismo muito importante para a segurança de dados é a assinatura digital, que garante a integridade dos dados por meio de criptografia, e seu acesso pode ser irrestrito e seu conteúdo não pode ser modificado [Alerta Security 2016].

Como as informações nas empresas são armazenadas em um Banco de Dados, faz-se necessário garantir a segurança lógica dos dados armazenados, contra revelação, alteração ou destruição não autorizadas. [Date 2000]. Para garantir essa segurança, são fornecidos privilégios diferentes para cada tipo de usuário, dependendo do cargo na

empresa, incluindo a capacidade de acessar arquivos específicos, podendo ler, inserir, alterar e excluir estes dados ou não. Privilégios esses fornecidos e de responsabilidade do Administrador de Banco de Dados (DBA), que poderá revogá-los a qualquer instante. Assim como os privilégios, o DBA também é responsável pelo monitoramento destes usuários, podendo-se utilizar de mecanismos para a proteção dos dados, como criação de logs, que registram todas as ações feitas pelos usuários dentro do Banco de Dados até o seu "Log off".

3. Auditoria em Banco de Dados

A auditoria em Banco de Dados consiste na realização sistemática de processos de exames das atividades desenvolvidas, com a finalidade de averiguar se estão de acordo com o que foi previamente planejado e estabelecido [Padoveze 2004]. Se tratando de Banco de Dados, a auditoria relaciona-se ao processo de identificação e a proteção do Banco de Dados contra pessoas que não são autorizadas a acessar algo ou todo o banco de dados. Com a auditoria de dados, é possível armazenar e examinar logs gerados pelo Sistema Gerenciador de Banco de Dados, com esses logs, é possível localizar usuários que estão fazendo alguma operação ilegal, por exemplo, visualizando dados que ele não está autorizado a visualizar.

A auditoria teve uma atenção especial devido a criação da lei Sarbanes-Oxley Atc (normalmente abreviada em SOX ou Sarbox) nos Estados Unidos em 30 de julho de 2002 pelo senador Paul Sarbanes e do deputado Michael Oxley. Essa lei foi criada para tentar segurar a saída de investidores, causada pela insegurança e perda de confiança, após uma série de fraudes e escândalos financeiros que atingiram várias empresas nos Estados Unidos, como Xerox, Enron, Tyco, WorldCom etc. A lei SOX exige a criação de mecanismos de auditoria e segurança confiáveis nas empresas, com o intuito explícito de evitar fraudes nos dados e identificá-las quando ocorrem, reduzindo assim os riscos nos negócios, dando credibilidade e transparência na gestão aos investidores [Portal de Auditoria 2017].

No mesmo ano, foi criado um conselho para supervisionar os processos de auditoria das empresas sujeitas a SOX, denominado Public Company Accounting Oversight Board (Conselho de Auditores de Companhias Abertas), no qual é responsável por estabelecer as normas de auditoria, controle de qualidade, ética e independência em relação aos processos de inspeção e a emissão dos relatórios de auditoria. Essas inspeções têm como objetivo, obrigar as empresas de auditoria a cumprir as regras estabelecidas.

O Administrador de Banco de Dados (DBA), geralmente é a pessoa responsável por efetuar a auditoria, dentre inúmeras atividades realizadas, a mais importante é o diagnóstico de problemas de execução do Sistema Gerenciador de Banco de Dados e o monitoramento das operações realizadas pelos usuários do sistema [Medeiros 2006]. O DBA tem como principal atividade, diagnosticar alterações indevidas e eventuais exclusões nos dados do sistema, para isso o Sistema Gerenciador de Banco de Dados deve dispor de mecanismos que dê permissão para realização dessas atividades conforme o nível de segurança.

Pode-se auditar um Banco de Dados com a implementação de Logs que gravam as operações realizadas em tabelas, permitindo futuramente a visualização desses logs. Esses logs são uma sequência de registros em uma tabela, atualizada com todas as operações efetuadas no banco. [Silberschatz e Korth 2005]. Também podemos realizar uma auditoria utilizando regras [Elmasri 2005]. Essas regras são criadas ou inseridas no Banco de Dados, gravando então as atividades em tabelas específicas. Este tipo de auditoria pode ser utilizado com comandos de manipulação (DML) ou comandos de definição (DLL), esta última conhecida como auditoria de mudanças de estrutura. No caso do Sistema Gerenciador de Banco de Dados Oracle, podemos auditá-lo de forma simples, habilitando o parâmetro AUDIT_TRAIL com o valor db_extended, que tem como tarefa, rastrear o uso de certos privilégios, execução de comandos SQL e o acesso a certas tabelas ou tentativas de logon. Você poderá especificar se fará auditoria destes eventos quando eles forem bem-sucedidos, quando falharem por falta de permissão ou ambos [Oracle 2016].

A Auditoria se faz necessária para garantir a segurança e examinar os logs gerados pelo Banco de Dados, com almejo de rastrear operações feitas em um determinado período. Caso tenha alguma operação ilegal ou não autorizada, através de log, é possível identificar qual usuário efetuou a operação.

4. Oracle Audit Vault

Uma opção de auditoria muito utilizada e flexível é a ferramenta Oracle Audit Vault (OAV), desenvolvida pela Oracle Corporation, ela atende os padrões internacionais de segurança da informação, norma ISO 1779 e de padrões de prevenções de fraudes, como a legislação norte-americana Sarbanes-Oxley, exigindo que os registros de auditoria em sistemas operacionais e em banco de dados se utilizem de um armazenamento inviolável.

O Oracle Audit Vault oferece um poderoso controle de segurança que ajuda a proteger os dados das aplicações de acessos não autorizados e cumpre os requisitos de privacidade regulamentares. Ele automatiza a consolidação e o monitoramento dos dados auditados de um Banco de Dados Oracle e outros Sistemas Gerenciadores de Banco de dados e fornece uma segurança interna robusta aos dados de auditoria consolidados por usuários privilegiados que administram o repositório do Oracle Audit Vault. Também fornece relatórios internos, que podem ser usados por auditores e equipe de segurança para monitorar de perto as atividades realizadas no banco de dados. Esses relatórios podem ser visualizados de forma dinâmica por um console, também podem ser agendados e enviados por e-mail para uma pessoa designada. Essas notificações são muito importantes para proatividade de eventos confidenciais [Oracle 2016].

A figura 1 mostra o funcionamento do Oracle Audit Vault, que, a partir de um Banco de Dados Oracle ou não Oracle, extrai os registros de log, salvando em sua própria base de dados, que é inviolável, entregando assim, informações íntegras e consistentes, e com esses logs, criar relatórios para tomada de decisões.

Figura 1. Funcionamento do Oracle Audit Vault

Fonte: Oracle, 2016

Os controles do Oracle Audit Vault podem ser implementados para bloquear o acesso a contas com altos privilégios para os dados de aplicação e controlar solicitações dentro do Banco de Dados utilizando a autorização por multifatores. O Oracle Audit Vault protege ambientes de banco de dados de forma transparente, eliminando o tempo e custo consumido pelas alterações nas aplicações, oferecendo controles de comunicação flexíveis e dinâmicos com a segurança do Banco de Dados.

Utilizando o Oracle Audit Vault, pode-se controlar contas do banco de dados, visto que as contas com níveis de privilégio altos são um dos caminhos mais utilizados para ganhar acessos a dados sensíveis e realizar atividades não autorizadas. Enquanto o acesso amplo facilita a manutenção do banco, ele também permite entregar uma quantidade maior de dados [Oracle 2016].

5. Auditoria Padrão

Assim como outros Sistemas Gerenciadores de Banco de Dados, o Oracle Database possuí o parâmetro de inicialização AUDIT_TRAIL que, se habilitado com o valor db_extended, tem a função de registrar atividades de auditoria, fornecendo informações sobre operações realizadas por usuários em quaisquer tabelas do Banco de Dados. Esses registros são armazenados em uma tabela de auditoria padrão, chamada DBA_AUDIT_TRAIL (a tabela SYS.AUD$) [Oracle 2016].

Este método de auditoria consiste em uma auditoria padrão, pois muitos dos dados armazenados são informados desorganizadamente, deixando difícil o entendimento das informações, além de não ser um método seguro, pois qualquer pessoa que tenha acesso a essa tabela pode simplesmente apagar seu conteúdo.

A Auditoria padrão não tem um sistema específico para gerar relatórios, ela traz somente informações geradas pelo próprio Banco de Dados, podendo somente ser exportadas para uma tabela em Excel por exemplo, não garantindo que as informações ali constadas foram alteradas após essa exportação. Os filtros aplicados para encontrar alguma informação específica contida nos registros são feitos através de comandos de busca com condições específicas.

6. Materiais e Métodos

Para a realização desse estudo, foi utilizado um notebook hospedeiro com o Software Oracle VirtualBox Versão 5.2.4 para a criação de duas máquinas virtuais. A primeira máquina virtual foi utilizada para a instalação do Oracle Audit Vault Server Versão 12.2.0.6.8, que foi escolhido por ser bem aceito no mercado, além de ser homologado para tal finalidade. Esta máquina virtual exige um espaço em disco de 250GB, e 2GB de memória. Foi necessário a configuração das máquinas na mesma rede, pois os servidores necessitaram estar na mesma faixa de IP para se comunicarem.

Por se tratar de um Sistema independente e fechado, o Oracle Audit Vault é gerenciado através de um navegador de internet, que demonstrou ter uma interface amigável e de fácil configuração e ajustes. Nesta interface, é possível fazer as configurações de acesso para a extração de registros de um Banco de Dados instalado em outro Servidor, também a realização de filtros para gerar relatórios específicos de Auditoria.

Na segunda máquina virtual foi utilizado um Banco de Dados Oracle 11g como fonte de extração de logs de auditoria. A escolha do Sistema Gerenciador de Banco de Dados Oracle 11G foi por ser um dos Sistemas Gerenciadores de Banco de Dados mais utilizados no mundo.

Para a obtenção automática de logs, foi necessário habilitar a auditoria padrão Oracle, que consiste em ativar o parâmetro AUDIT_TRAIL com o valor db_extended em seu sistema. Após isso, o Banco de Dados Oracle passou a gerar logs de auditoria por meio de scripts automáticos, que serão armazenados na tabela DBA_AUDIT_TRAIL (SYS.AUD$). A habilitação deste parâmetro afeta o desempenho da máquina, aumentando o consumo de I/O e CPU [Prado 2013].

O método de testes utilizado neste estudo foi feito baseando-se em consultas e alterações no Banco de dados, com o objetivo de gerar os registros de auditoria. Para a obtenção destas informações, utilizamos o Esquema HR, por se tratar de um Esquema padrão Oracle que contém dados e é utilizado com fins didáticos, ou seja, para demonstrações de recursos em sala de aula. Para facilitar a visualização dos resultados, foi criado o usuário FATECAUDIT, com privilégios suficientes para os testes realizados.

Por serem de fácil entendimento, além de maior foco de atenção nas auditorias, as ações abordadas neste estudo foram: Logon, Logoff, Select e Update, com o objetivo de gerar informações referentes as alterações realizadas no Banco de Dados, e assim, poder gerar relatórios utilizando uma auditoria padrão e compará-la com a auditoria realizada pelo Oracle Audit Vault.

7. Resultados obtidos

Após as ações Logon, Logoff, Select e Update realizadas no Banco de Dados, realizamos uma consulta na tabela DBA_AUDIT_TRAIL (SYS.AUD$) para a extração das informações de Auditoria Padrão.

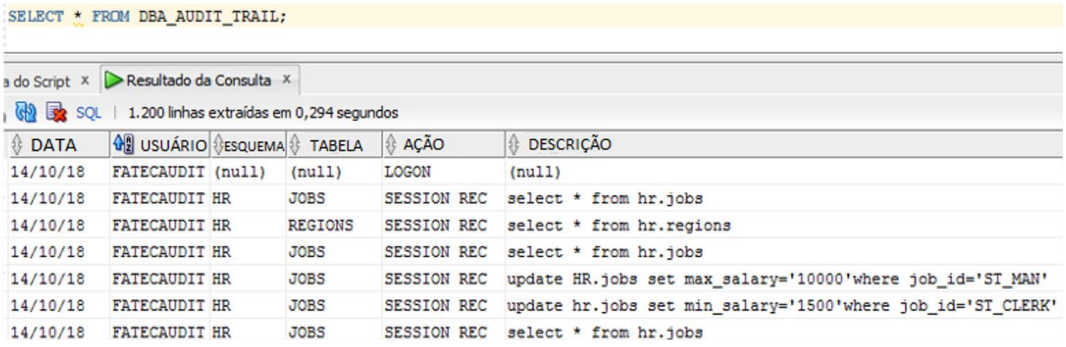
A auditoria consiste na coleta de dados onde vários campos são preenchidos com informações, porém nem todos os campos contém informações relevantes, como códigos internos da Oracle e valores em branco. Na tabela 1 podemos observar os campos mais relevantes no qual focamos e que foram coletados pela auditoria.

DATA	Data que foi realizada a ação do usuário
USUÁRIO	Usuário que realizou a ação
ESQUEMA	Esquema no qual as tabelas pertencem
TABELA	Tabelas utilizadas
AÇÃO	Ação realizada
DESCRIÇÃO	Descrição da ação realizada

Tabela 1. Informações fornecidas pelo Oracle SQL Developer

Fonte: Os Autores

Na figura 2, extraímos os registros obtidos em uma Auditoria Padrão realizada pelo Software Oracle SQL Developer.



```
SELECT * FROM DBA_AUDIT_TRAIL;
```

a do Script × | Resultado da Consulta ×

SQL | 1.200 linhas extraídas em 0,294 segundos

DATA	USUÁRIO	ESQUEMA	TABELA	AÇÃO	DESCRIÇÃO
14/10/18	FATECAUDIT	(null)	(null)	LOGON	(null)
14/10/18	FATECAUDIT	HR	JOBS	SESSION REC	select * from hr.jobs
14/10/18	FATECAUDIT	HR	REGIONS	SESSION REC	select * from hr.regions
14/10/18	FATECAUDIT	HR	JOBS	SESSION REC	select * from hr.jobs
14/10/18	FATECAUDIT	HR	JOBS	SESSION REC	update HR.jobs set max_salary='10000'where job_id='ST_MAN'
14/10/18	FATECAUDIT	HR	JOBS	SESSION REC	update hr.jobs set min_salary='1500'where job_id='ST_CLERK'
14/10/18	FATECAUDIT	HR	JOBS	SESSION REC	select * from hr.jobs

Figura 2. Auditoria padrão Oracle

Fonte: Os Autores

Neste método de auditoria, um problema que pode ser considerado grave é que, caso algum usuário tenha privilégios de acesso a tabela SYS.AUD$, ele simplesmente poderá apagar todos os registros executando comando de remoção dos registros, e prejudicando uma eventual auditoria.

A figura 3 mostra a primeira página do relatório gerado pelo Oracle Audit Vault, que analisa o percentual de transações de cada usuário no Banco de Dados de um determinado período, essa informação poderá identificar um usuário não autorizado que tenha realizado a conexão com o Banco de Dados.

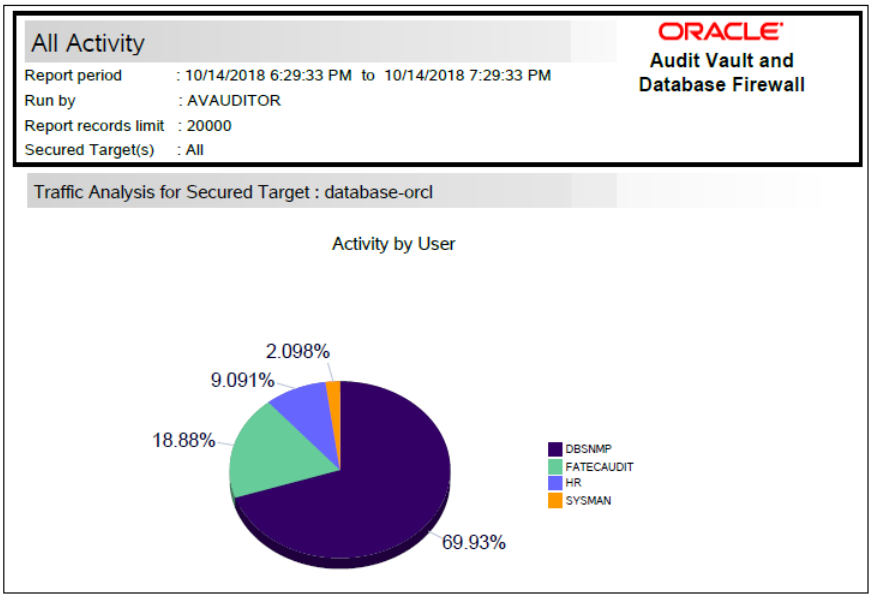


Figura 3. Relatório de Acesso Oracle Audit Vault

Fonte: Os Autores

Os dados obtidos na auditoria padrão, são extraídos automaticamente pelo Oracle Audit Vault. Esses logs de registros são armazenados em uma Base de Dados própria, que fica no Servidor do Oracle Audit Vault. Os resultados obtidos são entregues de forma simples, onde podemos filtrar por data, usuário, esquema etc. É importante destacar que pode-se auditar todos os esquemas, tabelas e colunas de um Banco de Dados.

A figura 4 mostra os eventos realizados no Banco de Dados em um determinado tempo de 3 minutos. Através dessas informações, podemos notar ações como, Logon, Logoff, Select e Update. Essas informações são muito importantes, pois nela conseguimos notar que o usuário FATECAUDIT fez alterações de Salário na tabela EMPLOYEES, e no caso, se ele não tivesse permissão para tal ação. O relatório serve como ponto de partida para uma possível tomada de decisão em relação a um usuário em seguida as providências de segurança devem ser tomadas onde uma delas seria o bloqueio ou as restrições de privilégio do usuário.

Event Time	Event Name	Event Status	User Name	Target Object	Client IP
Command Text					
10/14/2018 6:56:24 PM	SESSION REC	SUCCESS	FATECAUDIT	EMPLOYEES	
select * from hr.employees					
10/14/2018 6:56:31 PM	SESSION REC	SUCCESS	FATECAUDIT	REGIONS	
select * from hr.regions					
10/14/2018 6:56:32 PM	LOGON	SUCCESS	DBSNMP		fe80::552b:fb7d:bfc:e8b8%11
10/14/2018 6:56:32 PM	LOGOFF	SUCCESS	DBSNMP		
10/14/2018 6:56:42 PM	SESSION REC	SUCCESS	FATECAUDIT	JOBS	
select * from hr.jobs					
10/14/2018 6:56:55 PM	SESSION REC	SUCCESS	FATECAUDIT	EMPLOYEES	
select * from hr.employees					
10/14/2018 6:57:29 PM	SESSION REC	SUCCESS	FATECAUDIT	EMPLOYEES	
update hr.employees set salary='10000' where employee_id=206					

Figura 4. Relatório de Auditoria Oracle Audit Vault

Fonte: Os Autores

O resultado deste relatório nos traz informações satisfatórias, como alterações, visualizações e logins no Banco de Dados. As informações fornecidas por ele são, a data e hora que foi realizada tal ação, a ação realizada, se ela obteve sucesso ou não, o nome do usuário que a efetuou, a tabela que determinada ação foi realizada e o IP da máquina que acessou o Banco de Dados.

Podemos notar na figura 4 que as informações de IP somente são extraídas quando o usuário faz o Logon no Banco de Dados, exceto o usuário DBSNMP, que é um usuário padrão da Oracle, que fica monitorando o Banco de Dados, fazendo Logon e Logoff a todo momento.

É possível notar pela figura 5, em destaque vermelho, duas tentativas de acesso ao Banco de Dados do usuário FATECAUDIT utilizando senhas incorretas. Através dessas informações, o DBA conseguirá identificar pelo Internet Protocol (IP), qual máquina está tentando acessar o Banco de Dados com este usuário, e assim evitar acessos não autorizados, bloqueando e identificando quem efetuou tal tentativa.

Event Time	Event Name	Event Status	User Name	Target Object	Client IP
Command Text					
10/14/2018 6:40:02 PM	LOGOFF	SUCCESS	DBSNMP		
10/14/2018 6:40:17 PM	LOGON	SUCCESS	DBSNMP		fe80::552b:fb7d:bfc:e8b8%11
10/14/2018 6:40:17 PM	LOGOFF	SUCCESS	DBSNMP		
10/14/2018 6:40:33 PM	LOGOFF	SUCCESS	SYSMAN		
10/14/2018 6:41:32 PM	LOGON	SUCCESS	DBSNMP		fe80::552b:fb7d:bfc:e8b8%11
10/14/2018 6:41:32 PM	LOGOFF	SUCCESS	DBSNMP		
10/14/2018 6:42:10 PM	LOGON	FAILURE	FATECAUDIT		192.168.0.98
10/14/2018 6:42:16 PM	LOGON	FAILURE	FATECAUDIT		192.168.0.98

Figura 5. Relatório de Auditoria Oracle Audit Vault

Fonte: Os Autores

O Oracle Audit Vault extrai as informações instantaneamente da tabela SYS.AUD$ assim que uma ação é realizada no Banco de Dados, podendo então ser realizada uma limpeza constante da tabela, a fim de mantê-la sempre vazia e não ocasionar um aumento considerável no armazenamento do Banco de Dados.

	Desempenho I/O / CPU	**Usabilidade**	**Disponibilidade de Hardware**	**Investimento**	**Segurança**
Auditoria Padrão	14,09% 15,89%	Consultas para emissão de relatórios são feitas através de comandos SQL	Utilizado no próprio Servidor onde o SGBD está instalado	Não tem custo por ser um parâmetro padrão do SGBD	Não possui segurança pois os dados de auditoria são salvos em uma tabela do próprio banco de dados
Oracle Audit Vault	14,09% 15,89%	Possui Interface WEB amigável para emissão de relatórios	Necessário Servidor próprio para a Instalação do Software	$ 6.000 (Seis mil dólares) por núcleo de processador	Possui banco de dados próprio no qual é inviolável, só se consegue extrair informações através de relatórios

Tabela 2. Principais características dos métodos de Auditoria.

Fonte: Os Autores

Na tabela 2 listamos as principais características que obtivemos nos resultados. Na primeira coluna podemos observar que o desempenho de ambos os métodos causa impactos iguais, pois a carga de auditoria será inicialmente utilizada no Servidor que mantém o Banco de Dados. Na segunda coluna, observamos que as consultas para emissão de relatórios em uma Auditoria Padrão são efetuadas somente através de comandos SQL. No Oracle Audit Vault, são efetuadas através de uma interface web, que se mostrou muito amigável com seus filtros diversos, como selecionar período, usuário, tabela etc. Na terceira coluna, temos a disponibilidade de Hardware, no qual uma Auditoria Padrão só necessita de o parâmetro AUDIT_TRAIL estar habilitado no SGBD, sendo esta uma característica padrão de fábrica do SGBD Oracle, já o Oracle Audit Vault necessita de um servidor próprio para a instalação do Software, onde será interligado via rede ao Servidor do Banco de Dados para a coleta dos logs de auditoria.

Na quarta coluna, observamos que uma Auditoria Padrão não tem custo para utilização por ser um recurso do próprio SGBD. O Oracle Audit Vault tem o valor de $ 6.000 (Seis mil dólares) por núcleo de processador, mais o valor do servidor para a instalação do Software.

Na última coluna observamos que a Auditoria Padrão não entrega segurança necessária para auditorias mais severas, que são efetuadas normalmente em grandes empresas do ramo Financeiro, pois os logs de auditoria são salvos em uma tabela, podendo esta, ter os dados limpos por qualquer usuário com privilégios. No Oracle Audit Vault, contamos com uma base de dados inviolável, que funciona como um cofre para as auditorias coletadas do banco de dados, utilizando-a somente para armazenar os logs de auditoria e para emissão de relatórios, sendo impossível apagar os dados nela contidos.

8. Conclusão

O processo de auditoria efetuado pelo Oracle Audit Vault se mostrou muito seguro e eficiente comparado a uma auditoria padrão. Os dados nele armazenados, são íntegros, disponíveis e seguros. Estes dados contêm informações muito importantes para as empresas, pois com elas, pode-se tomar iniciativas para prevenir o acesso indevido de usuários maliciosos e não autorizados a acessar tal informação.

Com os registros de auditoria salvos no Oracle Audit Vault, temos a certeza de que nenhuma informação foi alterada de forma maliciosa, pois ele tem uma Base de Dados inviolável, exigido pela lei Sarbanes Oxley. Essa Base de Dados inviolável se torna essencial, porque as informações nela contidas, serão mais difíceis de serem contestadas em casos jurídicos.

Ao contrário da Auditoria efetuada por Softwares, uma Auditoria Padrão consiste em somente ter dados momentâneos para uma tomada de decisão que não expressa muita importância para uma empresa, pois esses dados poderão ser deletados a qualquer momento, não garantindo que as informações ali contidas serão integras, ou seja, que podem ter sido alteradas.

Por fim, concluímos que para uma Auditoria completa em um Banco de Dados, se faz necessário o uso de Softwares mais robustos e homologados para tal finalidade, pois esses Softwares entregarão de forma fácil e rápida, os relatórios necessários para

uma tomada de decisões e também, fornecer maior segurança das informações extraídas, garantindo assim sua integridade e confidencialidade.

Referências

Alerta Security (2016) “Segurança da Informação”. https://www.alertasecurity.com.br/blog/117-entenda-oque-e-seguranca-da-informacao-e-reduza-riscos-na-empresa, Março.

Bluephoenix (2018) “Boas práticas de segurança”. http://www.bluephoenix.pt, Março.

Date, C. J. (2000) “Introdução a sistemas de banco de dados”. Rio de Janeiro, Campus, 7ª edição.

Elmasri, N. (2005) “Sistemas de Banco de Dados”. São Paulo, Pearson, 4ª edição.

Medeiros, M. (2006) “Banco de Dados para Sistemas de Informação”. Rio de Janeiro, Visual Books, 1ª Edição.

Oracle (2016) “Oracle Audit Vault”. http://www.oracle.com/technetwork/pt/database/audit-vault/overview/index.html, Abril.

Padoveze, C. L. (2004) “Sistemas de Informações Contábeis”. São Paulo, Atlas, 4ª edição.

Portal de Auditoria (2017) “Introdução à Lei Sarbanes Oxley”. https://portaldeauditoria.com.br/introducao-lei-sarbanes-oxley-sox, Maio.

Prado. F (2013) “Auditoria X Performance no Oracle Database”. http://www.fabioprado.net/2013/01/auditoria-x-performance-no-oracle.html, Janeiro.

Silberschatz, A. e Korth, H. F. (2005) “Sistemas de Banco de Dados”. Rio de Janeiro, LTC, 4ª edição.