Argos: Solução Centralizada para Logging de Aplicações

Ezequiel Juliano Müller[1], Roberto Franciscatto[1], Antonio R. Delepiane de Vit[1]

[1]Colégio Agrícola de Frederico Westphalen (CAFW)
Universidade Federal de Santa Maria – RS (UFSM)
Caixa Postal: 54 – CEP: 98400-000 – Frederico Westphalen – RS – Brasil

ezequieljuliano@gmail.com, {roberto,rodrigodevit}@cafw.ufsm.br

Abstract. *Information is a key asset to any organization. Adopt appropriate measures logging application by means of a solution capable of providing an accurate analysis for help the decision-making process and that allows the resolution of the problems of day-to-day organizational, becomes a necessary and irreversible process. Thus, this paper has as objective to present the development of a centralized solution for managing logs of applications that can guarantee the security of information, detecting unauthorized activity or non-compliance with security policies for information systems.*

Resumo. *A informação é um ativo essencial para qualquer organização. Adotar medidas adequadas efetuando logging de aplicações por meio de uma solução capaz de fornecer uma análise precisa e que auxilie no processo de tomada de decisão, permitindo a resolução dos problemas do dia-a-dia organizacional, torna-se um processo necessário e irreversível. Desta forma, o presente artigo possui como objetivo apresentar o desenvolvimento de uma solução centralizada para a gestão de logs de aplicações, capaz de garantir a segurança da informação, detectando atividades não autorizadas ou em não conformidade com as políticas de segurança dos sistemas de informações.*

1. Introdução

A informação assume, nos dias de hoje, um papel fundamental e uma importância relevante para o funcionamento tático, estratégico e operacional de qualquer organização. Ela está presente e é fundamental em todos os níveis organizacionais e deve ser devidamente protegida. Neste sentido, a tarefa de *logging* de aplicações se destaca, pois os *logs* são fontes riquíssimas de informações que são gerados por servidores e aplicações a todo o momento que eventos significativos acontecem, possibilitando um verdadeiro rastreamento do processo de geração da informação. [Clemente 2008].

Devido a grande quantidade de informação que é gerada a todo o momento, os registros de *logs* tem se tornado ao longo dos últimos anos, verdadeiros aliados dos profissionais de TI, pois oferecem mecanismos de registros de eventos. Porém, a implementação destes mecanismos na maioria das vezes se constitui em uma tarefa complexa, pois para criar e gerenciar saídas de *logs* é necessária inclusão de comandos diretos no código fonte da aplicação, aumentando desta forma o tempo de desenvolvimento e a complexidade do código gerado. Além disso, existem outros problemas como o fato de não haver padrões para o conteúdo e formato dos arquivos de *logs* gerados, dificultando o seu uso por aplicações de análise, ou ainda o armazenamento dos *logs* na própria base de dados da aplicação, ocasionando perda de desempenho e possibilitando que o usuário possa negligenciar estas informações [Alves 2007].

Na sequência deste artigo são apresentados alguns conceitos relativos à segurança da informação e trabalhos relacionados ao tema (seção 2), a solução proposta (seção 3) e as conclusões finais (seção 4).

2. Segurança da Informação e Trabalhos Relacionados

O processo de gerar, armazenar e analisar registros de *logs* seja em servidores, em equipamentos de redes ou em qualquer tipo de sistema de informação é uma pequena parte de um processo muito maior denominado auditoria em sistemas de informação. Para compreender todo este processo é importante destacar a importância da informação para as organizações e como os *logs* atuam neste processo.

A informação é um bem de grande valor e como qualquer outro ativo de uma organização é essencial para os negócios e consequentemente deve ser protegida. E isto se torna importante ao passo que cada vez mais vivemos de forma interconectada. Como resultado desta interconexão as organizações e até mesmo as pessoas estão expostas a um crescente número e uma grande diversidade de vulnerabilidades. A informação existe em diversas formas e não importa qual for esta forma ou o meio onde ela é compartilhada é necessário que ela seja protegida de forma adequada [ABNT 2005].

É importante garantir a proteção dos dados, no sentido de preservar o valor que estes possuem para as organizações. Visando esta proteção é que os *logs* ganham destaque. Eles são gerados por qualquer aplicação – hoje qualquer tipo de sistema possui no mínimo ferramentas gerais para a geração de *logs*, possuindo como característica conter informações sobre eventos ocorridos para posterior verificação. Apesar de ser uma medida básica, os *logs* são considerados uma das formas mais elementares da auditoria de sistemas, pois oferecem uma visão das atividades que estão ocorrendo nos sistemas, possibilitando a análise ou detecção de problemas ou falhas, além de servir como evidência para investigações de algum incidente de segurança [Medeiros 2001].

Existem atualmente algumas ferramentas e trabalhos propostos na área do trabalho em questão que servem como modelo e possuem como premissa a incorporação do processo de *logging* em sistemas informatizados, bem como o gerenciamento e armazenamento centralizado de registros de *logs*.

Por exemplo, para a infraestrutura de desenvolvimento de *log* existem projetos (Log4j[29] e JLog[30]) que oferecem um conjunto de bibliotecas, as quais possuem operações para instanciar, configurar, formatar as saídas e envio das mensagens para o mecanismo de *log*. Estes projetos apenas geram as informações de *logs* e não possuem extensões que possibilitem a captura e armazenamento centralizado destas informações. Na área relacionada ao armazenamento e análise de *logs*, existem projetos (Scribe[31], Splunk[32] e LogZilla[33]), capazes de oferecer um mecanismo para a centralização de *logs*. Estas ferramentas possuem como foco principal realizar *logging* de redes de computadores, deixando um pouco a desejar quanto à necessidade de *logging* sobre aplicações comerciais, identificando principalmente alterações em banco de dados.

[29] http://logging.apache.org/log4j/2.x/
[30] http://jlog.org/
[31] https://github.com/facebook/scribe/wiki
[32] http://www.splunk.com/
[33] http://nms.gdd.net/index.php/LogZilla

3. Argos: Solução para Logging de Aplicações

O projeto proposto trata de uma solução especializada e centralizada para gestão de *logs* de aplicações capaz de garantir a segurança da informação, detectando atividades não autorizadas ou em não conformidade com a política organizacional, registrando e monitorando ocorrências de um estado da aplicação auditada em um único repositório, possibilitando que problemas sejam identificados e solucionados de maneira ágil.

A solução proposta, apresentada na Figura 1, é um *software* que possui a *web* como ambiente operacional, ou seja, vai executar na nuvem oferecendo um mecanismo para envio de registros de *logs* com um padrão pré-definido. A aplicação que vai integrar ao Argos deve gerar os *logs* e enviar os mesmos por meio de um *Webservice*. Este *logs* poderão conter atividades de usuários, exceções do sistema ou qualquer outro evento de segurança da informação. Posteriormente este *logs* poderão ser analisados e filtrados através de uma interface *web*. Outros aspectos são levados em consideração, como acesso seguro, possibilidade de montagem de filtros, *dashboards* e gráficos com informações cruciais além do envio automático de alertas quando houver *logs* críticos.

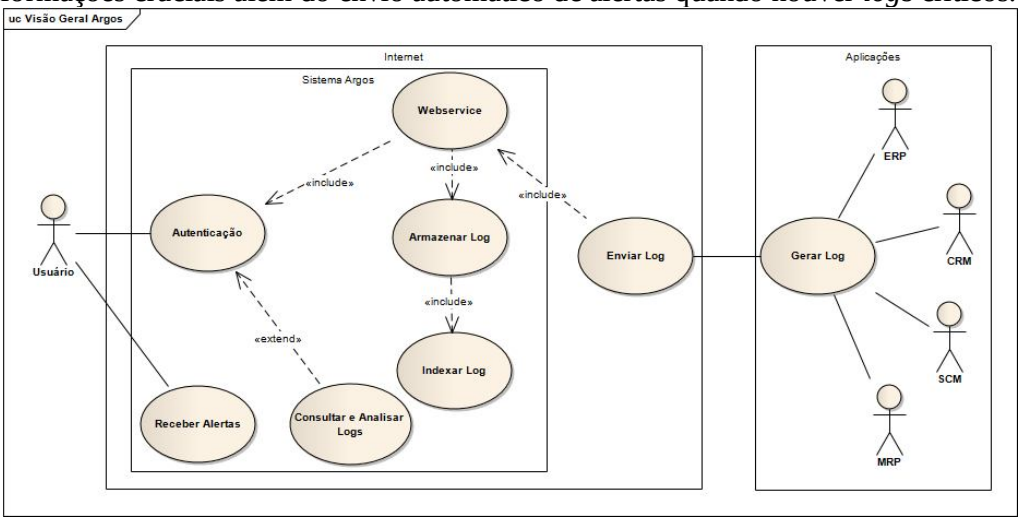

Figura 7. Visão Geral do Sistema Argos

Por se tratar de um *software* capaz de armazenar e processar grandes quantidades de dados faz-se necessário a utilização de tecnologias capazes de suprir toda esta demanda. Desta forma, tecnologias emergentes como o Demoiselle[34], que se trata de um *framework* integrador de diversas tecnologias especialistas Java, o Apache Cassandra[35], banco de dados *NOSQL* distribuído e altamente escalável e o Apache Lucene[36], biblioteca de mecanismo de procura de texto também altamente escalável, aparecem como boas alternativas *open source* (sem custo) para o desenvolvimento.

4. Conclusão

Considerada um ativo altamente significativo e essencial para os negócios de uma organização, a informação deve ser gerenciada e protegida com a adoção de medidas adequadas, principalmente em um ambiente de negócios cada vez mais interconectado.

[34] http://www.frameworkdemoiselle.gov.br/
[35] http://cassandra.apache.org/
[36] http://lucene.apache.org/core/

Garantir a segurança da informação significa dar continuidade aos negócios, minimizar riscos e ameaças e maximizar investimentos e oportunidades.

Quando a segurança da informação é negligenciada, ignorando o armazenamento de registros de *logs*, vários aspectos importantes como a confidencialidade, integridade e disponibilidade são afetados. Além disso, quando não é possível garantir que um usuário é de fato quem alega ser, o sistema perde a capacidade de provar que um usuário executou determinada ação e não se tem uma rastreabilidade de tudo o que foi realizado no sistema, impossibilitando a detecção de fraudes ou alterações indevidas. O *logging* é uma dimensão muito importante de uma aplicação e é extremamente importante reconhecer a sua aplicabilidade. O Argos possui como premissa garantir o seguro armazenamento de informações de *logs* administrando de forma objetiva os mesmos.

Devido ao fato de grande parte das organizações – em especial as *softwares houses*, carecerem de uma solução especializada e com repositório central para *logs* de aplicações, o desenvolvimento desta solução vem de encontro a esta necessidade, garantindo um maior monitoramento e análise dos eventos de segurança da informação, possibilitando uma tomada de decisão mais eficaz e proporcionando uma garantia de que problemas ou comportamentos anormais sejam identificados e atendidos com uma maior brevidade.

Referências

ABNT, Associação Brasileira De Normas Técnicas. Tecnologia da informação — técnicas de segurança — código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005. 120 p.

ALVES, Marcelo Pitanga. et al. Middlog: Uma infraestrutura de serviços de log de aplicações baseada em tecnologias de middleware. , 2007. Disponível em: <http://sbrc2007.ufpa.br/anais/2005/ST%2010-04%207301.pdf>. Acesso em: 29 set. 2012.

CLEMENTE, Ricardo Gomes. Uma arquitetura para processamento de eventos de log em tempo real. 2008. Tese (Mestrado em Informática) – PUC Rio de Janeiro. Rio de Janeiro - RJ. Disponível em: <http://www.maxwell.lambda.ele.puc-rio.br/Busca_etds.php?strSecao=resultado&nrSeq=12571@1>. Acesso em: 29 set. 2012.

MEDEIROS, Carlos Diego Russo. Segurança da Informação: Implantação de Medidas e Ferramentas de Segurança da Informação. 2001. Monografia (Graduação em Informática) UNIVILLE. Joinville - SC. Disponível em: <http://www.ivanfm.com/files/docs/TCE_Seguranca_da_Informacao.pdf>. Acesso em: 29 set. 2012.