6
Conclusão

Nesta dissertação, foram abordados os conceitos relativos ao gerenciamento de log. Foram apresentados os padrões de logs existentes e as atividades relacionadas ao gerenciamento de logs. Sendo assim, foi feita uma revisão sobre as principais publicações relacionadas ao gerenciamento de logs. Em seguida, foi apresentada a visão de logs como fluxos de eventos, sobre a qual são introduzidas as atividades de correlação .

Foram, então, estudados métodos de correlação de eventos, presentes em diferentes linhas de pesquisa. O foco desta dissertação foi direcionado para métodos baseados em regras e métodos baseados em consultas. Para o caso dos métodos baseados em consulta, uma classe de sistemas, conhecida como *Data Stream Management Systems*, foi estudada.

Após a apresentação desta base conceitual, foram levantados os requisitos de um sistema de gerenciamento de logs, tendo em vista a realidade de uma empresa de *Internet.* O entendimento dos requisitos levou à procura de uma arquitetura adequada, onde foi escolhido o padrão de arquitetura orientada a eventos (EDA).

Por fim, foi desenvolvido um protótipo focado nas atividades de correlação de eventos de log. Sobre este protótipo, um cenário de uso com logs e situações reais foi criado, para que uma prova de conceito fosse realizada. Os testes sobre este cenário utilizaram arquivos de logs reais e identificaram duas situações de importantes como exemplos de análise em tempo real.

Ficou claro também que muitas outras situações interessantes também poderiam ser expressas através de regras de correlação ou de consultas contínuas. Desta forma, funcionalmente o protótipo desenvolvido atendeu as expectativas.

Nesse sentido, como conclusão do trabalho, pode-se dizer que a arquitetura apresentada é forte candidata a ser utilizada em empresas que possuem um grande volume de arquivos logs e precisam correlacionar a informação presente nestes arquivos para gerar conhecimento e ações em tempo real. O fato de ser baseada em ferramentas de código aberto facilita ainda mais a sua adoção. A expectativa é que deste protótipo nasça um projeto de

código aberto que tenha todo o código desenvolvido disponível e uma documentação com guias para instalação e indicações para parametrização do sistema.

É esperado também que este protótipo venha a gerar um projeto na Globo.com para a implementação de um sistema em produção capaz de realizar a correlação em tempo real de eventos. A expectativa é que este projeto seja iniciado ainda neste ano.

Como possíveis trabalhos futuros pode-se citar:

- Pesquisa e desenvolvimento dos demais nós da arquitetura, como os nós de visualização, armazenamento e pesquisa.
- Pesquisa e implementação de algoritmos capazes de aprender padrões interessantes sobre os eventos e adaptar ou criar regras de correlação.
- Pesquisa sobre a aplicação da arquitetura orientada a eventos e as ferramentas de correlação por regras e consultas aplicadas a outras áreas como aplicações financeiras e processos de negócio.