FACULDADE DE TECNOLOGIA SENAC GOIÁS
Segurança da Informação

Aldo Brito
Leniker Lettierre
Matheus Mello
Rony Carneiro

REGISTROS DE LOGS

Olegario Correa Neto

GOIÂNIA,
2017

Aldo Brito
Leniker Lettierre
Matheus Mello
Rony Carneiro

REGISTROS DE LOGS

Relatório apresentado como requisito parcial para obtenção de aprovação no Projeto Integrador, no Curso de Segurança da Informação, na Faculdade de Tecnologia Senac Goiás.

Olegario Correa Neto

GOIÂNIA,
2017

SUMÁRIO

1 GERAÇÃO DE LOGS

Geração de logs é o procedimento pelo qual um sistema operacional ou aplicativo registra eventos à medida que eles acontecem e preserva esses registros para posterior análise. Os registros de log fornecem a única evidência real de que um crime realmente aconteceu. Os arquivos de logs são essenciais para a notificação de incidentes, pois são capazes de armazenar diversas informações importantes, como a data e o horário em que uma determinada atividade ocorreu, o fuso horário, o endereço IP de origem da atividade, os dados completos que foram enviados, alterados ou excluídos e o resultado da atividade (se ela ocorreu com sucesso ou não).

A geração de logs é a geração de registros de eventos ou estatísticas para prover informações sobre a utilização e performance de um sistema, ou seja, são muito importantes para a administração segura de sistemas, pois possuem como premissa registrar informações sobre o seu funcionamento e sobre eventos por ele detectados. Na maioria das vezes, os logs são o único recurso que um administrador possui para descobrir as causas de um problema ou um comportamento anormal.

Qualquer registro de log gerado por um sistema pode ajudar a descobrir problemas na execução de softwares, problemas de hardwares, tentativas de invasão, acessos indevidos, entre outras coisas. Neste sentido, é importante manter estes registros seguros e intactos, pois em uma eventual auditoria de sistemas estes logs serão importantes. Portanto, a integridade e disponibilidade dos logs são fatores vitais para garantir a continuidade dos negócios. Neste cenário destacam-se as ferramentas que unificam a administração destes registros, pois possibilitam gerenciar redes e sistemas informatizados mais complexos.

Por meio dos arquivos de log é possível registrar ações dos usuários, o que os torna uma ótima fontes de informação para auditorias futuras. Os logs registram quem acessou os recursos computacionais, aplicativos, arquivos de dados e utilitários, quando foi feito o acesso e que tipo de operações foram efetuadas.

Desta forma, é possível identificar um invasor ou usuário não autorizado que realizou acesso a um determinado sistema, apagou ou alterou dados, acessou aplicativos, mudou configurações do sistema operacional com o intuito de prejudicar a organização e facilitar futuras invasões. Sem os registros de logs, estas ações não seriam identificadas fazendo com que o administrador sequer ficasse sabendo que houve uma invasão.

Uma auditoria de segurança bem-sucedida depende da existência de registros de logs íntegros e confiáveis. Independentemente do quão seguro é um computador, uma rede ou um sistema, nunca será possível confiar totalmente nos registros de um sistema que foi comprometido, pois isso dificulta ou até mesmo impossibilita uma auditoria de sucesso. Quando os registros de auditoria estão seguros é possível aumentar as chances de sucesso ao

se correlacionar e identificar padrões ou rever os incidentes de segurança ocorridos em um sistema. Para alcançar estes objetivos é recomendável estabelecer um sistema de logs centralizado e dedicado, ou seja, que tenha como função exclusiva a coleta, registro e análise de eventos de logs.

Devido ao fato de armazenar dados gerados pelo sistema, aplicações, rede, atividades dos usuários, entre outros, os logs fornecem inúmeras informações que se transformam em indicadores capazes de medir os níveis de segurança e de avaliar se medidas de segurança estão surtindo o efeito esperado e planejado. A melhor forma de verificar a extensão de um incidente de segurança, identificando que ativo foi violado e que a informação foi exposta é por meio dos registros de logs, por isso eles são vitais para a continuidade dos negócios de uma organização. Neste ponto, é importante ressaltar quanto ao uso correto dos softwares de análise de logs, pois estes registros são gerados de diversas formas e devem ser interpretados corretamente, possibilitando uma compactação e consolidação das informações no sentido de melhorar a extração do resultado final.

1.1 AUDITORIA DE LOGS

Auditar se faz necessário para certificar que as atividades dos usuários e administradores, falhas, exceções e eventos de segurança da informação estejam em conformidade com as regras de negócio e políticas (incluindo segurança da informação) estabelecidas pela empresa, além de certificar a eficácia das normas estabelecidas.

A análise de logs muitas vezes é tratada como uma tarefa de baixa prioridade pelas organizações e administradores de redes e sistemas, em muitos casos, os administradores sequer possuem recursos e treinamento para análises proativas, ou não os utilizam, por considerarem essa atividade “entediante” e menos importante que a resolução de problemas operacionais. A análise de logs acaba sendo uma atividade simplesmente reativa e improdutiva, onde se espera por uma falha ou desastre (as vezes levando a parada do total de um negócio) para solucionar um problema que em muitos casos estava sendo anunciado e “embaixo dos nossos olhos”.

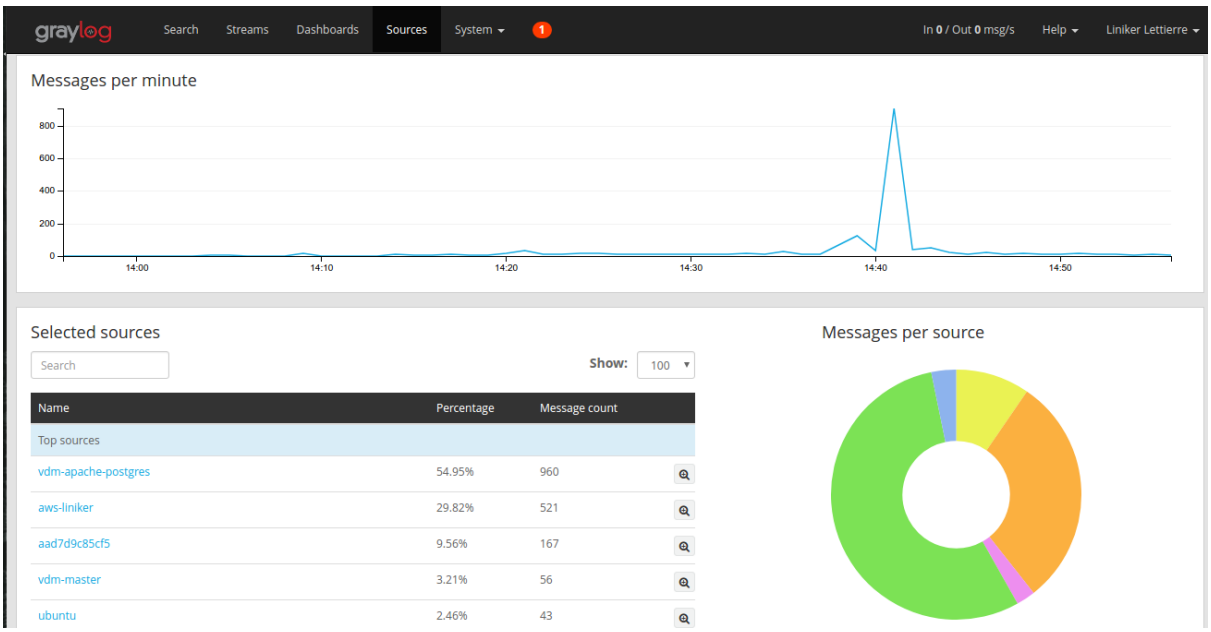
1.2 GRAYLOG

Uma ótima ferramenta para realizar coleta e análise de log é o GrayLog, ele é um concentrador de LOG, todos os LOG do servidor está sendo enviados para ele, incluindo Apache e Postgres.

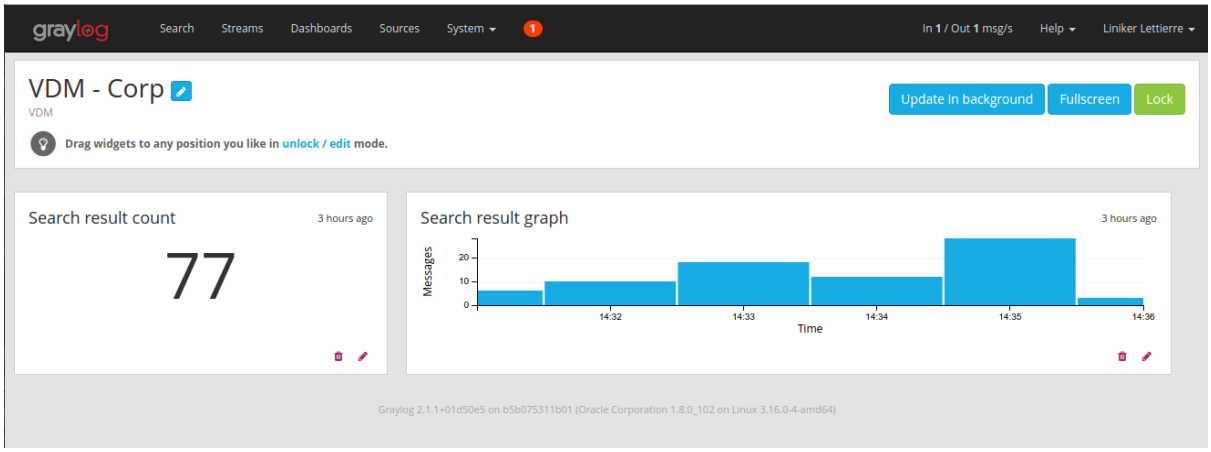
A grande vantagem de utilizar o Graylog é que além dele ser um concentrador de LOG ele também analisa os logs e com ele é possível realizar buscas avançadas nos LOG, Ativar alertas quando um determinado padrão acontecer, por exemplo tentativas falhas de conexão no usuário do Postgres, ou erros de Injeção de código malicioso nos sistemas WEB, É possível controlar tudo pela interface WEB do GrayLog, configurar novos tipos de Inputs,

verificar o uso de memória do servidor de LOG, personalizar o dashboard para mostrar gráficos e alertas.

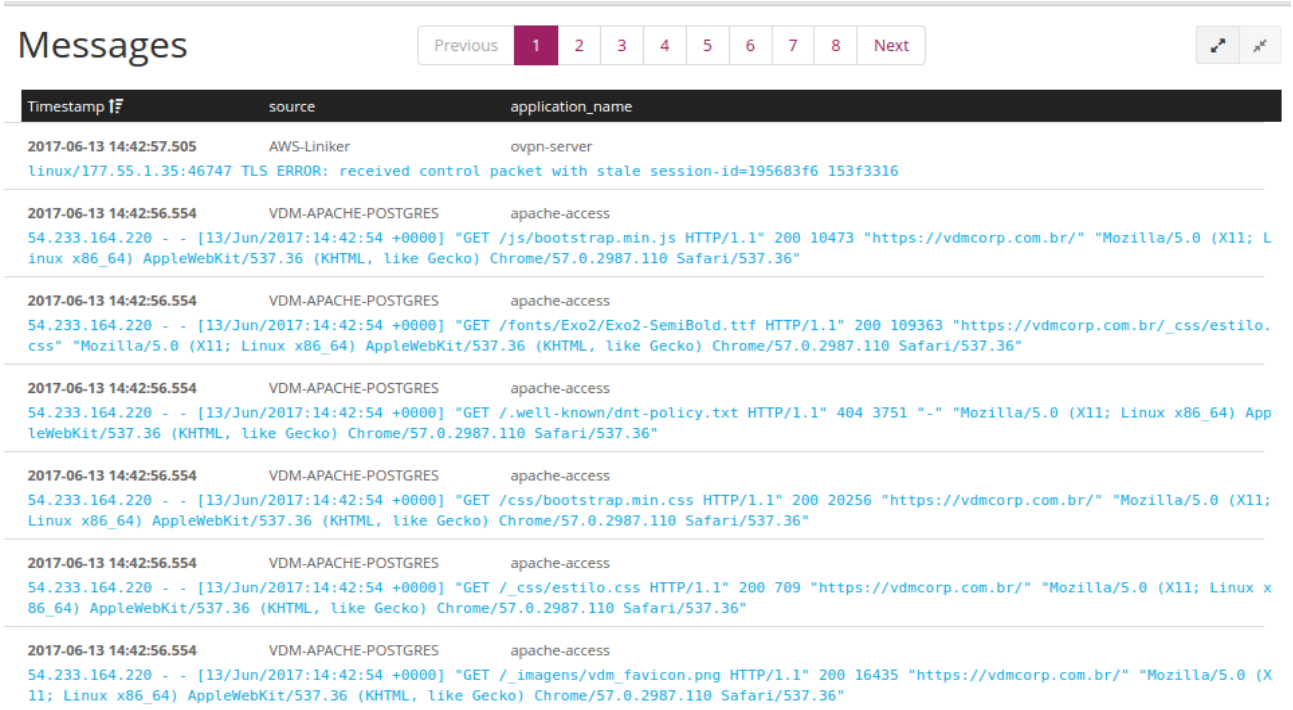
Nesta tela é informado a origem dos LOG e sua porcentagem sob o total,



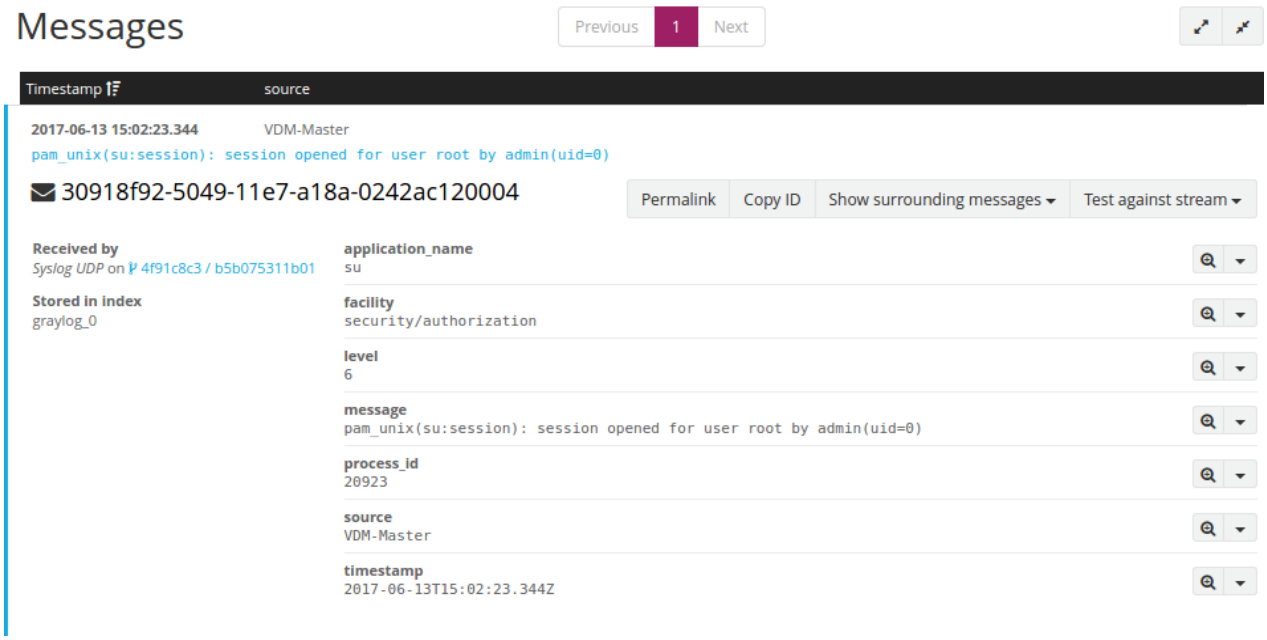
Exemplo de dashboard



Log recebido:



Log maximizado para ver com mais detalhes:



Infraestrutura;

GrayLog é uma ótima ferramenta para análise de LOG mas para isto ele necessita de bastante recurso computacional. O servidor está hospedado na Google Cloud.

Plataforma de processamento: Intel Haswell

Memória ram: 4GB

Armazenamento: 30GB em SSD

O envio dos logs é feito sob o protocolo TCP, assim garante que nenhum LOG será perdido no caminho,

Este GrayLog foi instalado usando Docker, foi usado a imagem original disponibilizada pelos desenvolvedores do GrayLog. Assim é possível migrar facilmente este sistema para outro servidor em poucos minutos.

Código do docker-compose:

```
version: '2'
services:
  vdm-mongo:
    image: "mongo:3"
    volumes:
      - /graylog/data/mongo:/data/db
  vdm-elasticsearch:
    image: "elasticsearch:2"
    command: "elasticsearch -Des.cluster.name='graylog'"
    volumes:
      - /graylog/data/elasticsearch:/usr/share/elasticsearch/data
  graylog:
    image: graylog2/server:2.1.1-1
    volumes:
      - /graylog/data/journal:/usr/share/graylog/data/journal
      - /graylog/config:/usr/share/graylog/data/config
    environment:
      GRAYLOG_PASSWORD_SECRET: Vasdkfj!@!@$&$@Wpadf1@!$#*A
      GRAYLOG_ROOT_PASSWORD_SHA2: b6959akdfj2342dasdf6s56d98a6sc522b44eecaf9b9675b1dc7
      GRAYLOG_WEB_ENDPOINT_URI: http://log.vdmcorp.com.br:9000/api
    links:
      - vdm-mongo:mongo
      - vdm-elasticsearch:elasticsearch
    ports:
      - "9000:9000"
      - "12201/udp:12201/udp"
      - "1514/udp:1514/udp"
      - "1514/tcp:1514/tcp"
```

Também foi utilizado um container Docker dedicado em capturar os LOG do apache e do Postgres e enviar para o GrayLog.

REFERÊNCIAS BIBLIOGRÁFICAS

https://respirandolinux.com.br/tag/auditoria-de-logs

http://www.ezequieljuliano.com.br/?p=76

https://hub.docker.com/r/graylog2/server/

https://gnulinuxbr.wordpress.com/2009/09/10/configurando-o-rsyslog-clienteservidor/

https://www.loggly.com/ultimate-guide/centralizing-apache-logs/