Aula 31 - Arquivos de Registros (LOGS)

Juliana Camilo Inácio

Instituto Federal de Santa Catarina
Campus São José

juliana.camilo@ifsc.edu.br

22 de Outubro de 2013

Introdução

- Arquivos de *log* são registros de atividades executadas no computador, geralmente por serviços específicos.
- Como administrador de sistemas o *log* do sistema é o seu melhor amigo.
- Se monitorá-lo cuidadosamente, você saberá com antecedência quando alguma coisa estiver errada com o sistema e, assim poderá resolver a maioria dos problemas antes que eles surjam.

Introdução

- Infelizmente, sua tarefa de monitorar todos os arquivos de *logs* aumenta conforme o número de servidores que você tem que administrar.
- Por isto, muitas vezes os administradores de sistemas usam softwares de processamento de *logs*, que podem ser configurados para alertá-los em certos eventos.
- Ou ainda, você administrador de redes (com conhecimento em programação), pode desenvolver sua própria ferramenta de análise de arquivos de *logs*.

Introdução

- Os *logs* geralmente ficam em /var/log e após seu servidor ter funcionado por um tempo, você perceberá que existem diversas versões antigas dos arquivos de log neste diretório, onde muitos deles são comprimidos com gzip.

Arquivos de LOG Importantes

- /var/log/syslog : registro geral do sistema.
- /var/log/auth.log : registro de autentificação do sistema.
- /var/log/mail.log : registro de e-mails do sistema.
- /var/log/messages : registro de mensagens gerais.
- /var/log/dmesg: registro de mensagens do kernel, geralmente a partir da inicialização do sistema.

Arquivos de LOG Importantes

Os logs que serão registrados no sitema são configurados no arquivo (para distribuição Ubuntu):

- /etc/rsyslog.d/50-default.conf

Arquivos de LOG Importantes

- A forma mais comum pela qual os programas registram as informações é através do daemon syslogd.
- **daemon:** programa de computador que roda de forma independente em background, ao invés de ser controlado diretamente por um usuário.

Arquivos de LOG Importantes

Configurando o syslogd:

- Entrar no arquivo /etc/rsyslog.d/50-default.conf
- Dentro deste arquivo, os *logs* serão configurados da seguinte forma:
  - recurso.nível de registro ação/caminho onde é salvo o arquivo de log

Arquivos de LOG Importantes

Tipos de recurso:

- kernel
- auth
- cron
- mail
- outros programas.

Arquivos de LOG Importantes

Tipos de níveis de registro:

- emerg: o sistema está inutilizável
- alert: uma ação deve ser tomada imediatamente
- crit: condições críticas
- err: condições de erro
- warning: mensagens de advertência
- notice: algo que merece investigação
- info: mensagens informativas
- debug: depuração

Arquivos de LOG Importantes

Tipos de ações:

- nome do arquivo: grava a mensagem no arquivo (endereço absoluto)
- @nomedohost/ipdohost: Encaminha a mensagem para um syslog em outra máquina
- usuário1,usuário2: Imprime as mensagens na tela do usuário se ele estiver logado

Informações Úteis

No Ubuntu também é possível analisar os *logs* através da interface gráfica.

- Sistema → administração → visualizador de arquivos de *log*
- ou no campo de pesquisa dos programas instalados, procure por **log**

Informações Úteis

Lembrando que existem softwares que analisam os arquivos de *logs* gerados, e que estes facilitam o trabalho do administrador da rede.