O que você precisa saber sobre Log na certificação LPI nível 1

A necessidade de registrar as atividades dos usuários e serviços dos sistemas é muito importante para os administradores a fim de mantermos um certo controle sobre as situações que ocorrem no nosso servidor. Os arquivos de logs ficam em **/var/log** e registram tudo o que acontecem com o kernel, com os daemons e utilitários do sistema.

Veja o que se pode obter com a ajuda de logs:

- Identificação dos usuários;
- Datas e horários de entrada (login, logout);
- Identidade do terminal, nome da máquina ou IP;
- Registro das tentativas de acesso aos aceitos e rejeitados;

O servidor de log utilizado no Linux é o **SysLog. Seu arquivo de configuração é o /etc/syslog.conf.**

Já existe uma versão mais atual que se chama **Syslog-ng** (new generation – nova geração), ele possui novas funcionalidades (arquivo de configuração **/etc/syslog-ng/syslog-ng.conf**).

O arquivo **syslog.conf** obedece algumas regras:

facilidade: É usada para especificar que tipo de programa está enviando a mensagem;
nível: Especifica o nível de gravidade da mensagem;
destino: O destino das mensagens pode ser um arquivo, um pipe (se iniciado por um "**|**"), um computador remoto (se iniciado por uma "**@**"), determinados usuários do sistema (especificando os logins separados por vírgula) ou para todos os usuários logados via wall (usando "*"");

A facilidade e o nível são separadas por um "**.**" e contêm parâmetros que definem o que será registrado nos arquivos de log do sistema:

auth: Mensagens de segurança/autorização (é recomendável usar authpriv em vez desse).
authpriv: Mensagens de segurança/autorização (privativas).
cron: Daemons de agendamento (cron e at).
daemon: Outros daemons do sistema que não possuem facilidades específicas.
ftp: Daemon de ftp do sistema.
kern: Mensagens do kernel.
lpr: Subsistema de impressão.
local0 a **local7**: Reservados para uso local.
mail: Subsistema de e-mail.
news: Subsistema de notícias da USENET.
security: Sinônimo para a facilidade auth (evite usá-la).
syslog: Mensagens internas geradas pelo syslogd.
user: Mensagens genéricas de nível do usuário.
uucp: Subsistema de UUCP.
*****: Confere com todas as facilidades.

Níveis

emerg: O sistema está inutilizável.
alert: Uma ação deve ser tomada imediatamente para resolver o problema.
crit: Condições críticas.
err: Condições de erro.
warning: Condições de alerta.
notice: Condição normal, mas significante.
info: Mensagens informativas.
debug: Mensagens de depuração.
***:** Confere com todos os níveis.
none: Nenhuma prioridade.

Rotacionamento de LOGS

O arquivo de configuração do rotacionamento é o **/etc/logrotate.conf** (no Red Hat o arquivo usado é o **/etc/rotate.conf**).

Arquivos e suas funções:

/var/log/dmesg	Arquivo que contém as mensagens da inicialização do sistema, pode ser visto com o comando **dmesg**.
/var/log/boot.log	Arquivo que contém as mensagens da inicialização do sistema.
/var/log/wtmp	É um arquivo binário que guarda dados (data, hora e terminal) das sessões de cada usuário. Como é um arquivo binário não pode ser lido diretamente com um editor de textos por exemplo. Esse arquivo costuma crescer muito. O comando **`last`** utiliza este arquivo.
/var/run/utmp	É um arquivo binário que guarda dados (data, hora e terminal) somente última sessão de cada usuário. Como é um arquivo binário não pode ser lido diretamente com um editor de textos por exemplo. O comando **`who`** ou **`w`** este arquivo.
/var/log/btmp	É um arquivo binário que guarda informações sobre as tentativas de login mal sucedidas. Seu conteúdo é visualizado com o comando **lastb**
/var/log/messages	Arquivo responsável pelos logs do sistema. Dica para visualizar as últimas mensagens do kernel: **# tail -f /var/log/messages**

Comandos:

dmesg	Mostra as mensagens ocorreram durante o boot. **# dmesg**
last	O comando `last` usa o arquivo **/var/log/wtmp** para gerar sua listagem. Exemplos do seu uso: **# last** - Mostra a listagem geral **# last tty1** - Mostra todas as atividades no tty1 **# last leonardo** - Mostra todas as atividades do usuário leonardo
lastb	informações sobre as tentativas de login mal sucedidas. O comando **who** ou **w** mostra essas tentativas.
lastlog	Mostra o último login dos usuários cadastrados no sistema. Usa o arquivo **/var/log/lastlog**