

Logs e arquivos .conf

Logs e arquivos de configuração em GNU/Linux

O que é um log?

- Estes arquivos de registros são chamados de logs e contém a data, hora e a mensagem emitida pelo programa (violações do sistema, mensagens de erro, alerta e outros eventos) entre outros campos.
- Enfim, muitos detalhes úteis ao administrador tanto para acompanhar o funcionamento do seu sistema, comportamento dos programas ou ajudar na solução e prevenção de problemas.

Diretórios

- Diretório padrão:
 /var/log
- Opcionalmente podem se encontrar em outros diretórios

Formato do arquivo de log

- Um arquivo de log é normalmente composto pelos seguintes campos:
 - Data|Hora|Máquina|daemon|mensagem

Daemons

- Em Unix e outros sistemas operacionais multitarefas, um daemon, acrônimo de Disk And Execution MONitor (Monitor de Execução e de Disco), é um programa de computador que roda de forma independente em background, ao invés de ser controlado diretamente por um usuário. Tipicamente, daemons têm nomes que terminam com a letra "d"; por exemplo, `syslogd` é o daemon que gerencia o log do sistema ("system log").

Syslogd e rsyslogd

- O gerenciador de logs pode ser o syslogd e o rsyslogd. Dependendo da distribuição.
- Na distribuição Ubuntu é utilizado o rsyslogd
- Os arquivos de configuração estão localizados em:
 - /etc/rsyslog.d/

Comandos importantes

- `cat`
 - `Cat [opções] arquivos`
 - Este comando envia o conteúdo de um ou mais arquivos para a saída padrão ou para um outro arquivo.

Comandos importantes

- less
 - less [opções] [arquivo]
 - Este comando permite fazer a paginação de arquivos ou da entrada padrão.

Comandos importantes

- tail
 - tail [opções] arquivo
 - Este comando exibe as últimas linhas de um arquivo texto.
- Obs: -f : continua indefinidamente tentando ler caracteres ao final do arquivo, assumindo que o arquivo está crescendo.

Logs importantes

- `/var/log/syslog` : General system log
- `/var/log/messages` : General log messages
- `/var/log/boot` : System boot log
- `/var/log/auth.log` : User login and authentication logs
- `/var/log/kern.log` : Kernel log file

- `/var/log/proftpd/proftpd.log` → Log de aplicação

Comandos Importantes

- Otimizando as buscas:

```
grep -i "fatal" /var/log/*
```

Comunicando com o daemon de logs

- Pode ser interessante gravar ocorrências diretamente nos Logs, um script ou programa que você crie por exemplo.
- Para gravar diretamente nos logs usamos o comando logger
 - logger “testando o servidor de log”
- Essa entrada estará provavelmente em `/var/log/syslog`