Guia Foca GNU/Linux
Capítulo 17 - Arquivos e daemons de Log

A atividade dos programas são registradas em arquivos localizados em `/var/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.
Alguns programas como o `Apache`, `exim`, `ircd` e `squid` criam diversos arquivos de log e por este motivo estes são organizados em sub-diretórios (a mesma técnica é usada nos arquivos de configuração em `/etc`, conforme a padrão FHS atual).

17.1 Formato do arquivo de log

Um arquivo de log é normalmente composto pelos seguintes campos:

`Data|Hora|Máquina|daemon|mensagem`

O campo *máquina* é o nome do computador que registrou a mensagem (a máquina pode atuar como um servidor de logs registrando mensagens de diversos computadores em sua rede). O campo *daemon* indica qual programa gravou a *mensagem*.
O uso dos utilitários do console pode ajudar muito na pesquisa e monitoração dos logs, por exemplo, para obter todas as mensagens do daemon `kernel` da estação de trabalho `wrk1`, eliminando os campos "wrk1" e "kernel":

```
cat /var/log/*|grep 'wrk1'|grep 'kernel'|awk '{print $1 $2 $3 $6 $7 $8 $9 $10 $11 $12}'
```

Os parâmetros "$1", "$2" do comando `awk` indica que campos serão listados, (omitimos $4 e $5 que são respectivamente "wrk1" e "kernel").

17.2 Daemons de log do sistema

Os daemons de log do sistema registram as mensagens de saída do kernel (`klogd`) e sistema (`syslogd`) nos arquivos em `/var/log` .
A classificação de qual arquivo em `/var/log` receberá qual tipo de mensagem é controlado pelo arquivo de configuração `/etc/syslog.conf` através de*facilidades* e *níveis* (veja Arquivo de configuração `syslog.conf`, Seção 17.2.1.1 para detalhes).

17.2.1 syslogd

Este daemon controla o registro de logs do sistema.

`syslogd [`*`opções`*`]`
opções

-f

Especifica um arquivo de configuração alternativo ao `/etc/syslog.conf`.
-h

Permite redirecionar mensagens recebidas a outros servidores de logs especificados.

-l [computadores]

Especifica um ou mais computadores (separados por ":") que deverão ser registrados somente com o nome de máquina ao invés do FQDN (nome completo, incluindo domínio).

-m [minutos]

Intervalo em *minutos* que o syslog mostrará a mensagem `--MARK--`. O valor padrão padrão é 20 minutos, 0 desativa.
-n

Evita que o processo caia automaticamente em background. Necessário principalmente se o `syslogd` for controlado pelo `init`.
-p [soquete]

Especifica um soquete UNIX alternativo ao invés de usar o padrão `/dev/log`.
-r

Permite o recebimento de mensagens através da rede através da porta UDP 514. Esta opção é útil para criar um servidor de logs centralizado na rede. Por padrão, o servidor `syslog` rejeitará conexões externas.
-s [domínios]

Especifica a lista de domínios (separados por ":") que deverão ser retirados antes de enviados ao log.

Na distribuição `Debian`, o daemon `syslogd` é iniciado através do script `/etc/init.d/sysklogd`.

17.2.1.1 Arquivo de configuração `syslog.conf`

O arquivo de configuração `/etc/syslog.conf` possui o seguinte formato:

```
facilidade.nível destino
```

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

- `facilidade` - É usada para especificar que tipo de programa está enviando a mensagem. Os seguintes níveis são permitidos (em ordem alfabética):
- `auth` - Mensagens de segurança/autorização (é recomendável usar authpriv ao invés deste).
- `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 usa-la).
- `syslog` - Mensagens internas geradas pelo `syslogd`.
- `user` - Mensagens genéricas de nível do utilizador.
- `uucp` - Subsistema de UUCP.
- `*` - Confere com todas as facilidades.

  Mais de uma facilidade pode ser especificada na mesma linha do `syslog.conf` separando-as com ",".
- `nível` - Especifica a importância da mensagem. Os seguintes níveis são permitidos (em ordem de importância invertida; da mais para a menos importante):
- `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.

  Além destes níveis os seguintes sinônimos estão disponíveis:

- `error` - Sinônimo para o nível err.
- `panic` - Sinônimo para o nível emerg.
- `warn` - Sinônimo para o nível warning.
- `destino` - O destino das mensagens pode ser um arquivo, um pipe (se iniciado por um "|"), um computador remoto (se iniciado por uma "@"), determinados utilizadores do sistema (especificando os logins separados por vírgula) ou para todos os utilizadores logados via `wall` (usando "*").

Todas as mensagens com o nível especificado e superiores a esta especificadas no `syslog.conf` serão registradas, de acordo com as opções usadas. Conjuntos de *facilidades* e *níveis* podem ser agrupadas separando-as por ";".
OBS1: Sempre use TABS ao invés de espaços para separar os parâmetros do `syslog.conf`.
OBS2: Algumas facilidades como `security`, emitem um beep de alerta no sistema e enviam uma mensagem para o console, como forma de alerta ao administrador e utilizadores logados no sistema.

Existem ainda 4 caracteres que garantes funções especiais: "*", "=", "!" e "-":

- "*" - Todas as mensagens da *facilidade* especificada serão redirecionadas.
- "=" - Somente o *nível* especificado será registrado.
- "!" - Todos os *níveis* especificados e maiores NÃO serão registrados.
- "-" - Pode ser usado para desativar o sync imediato do arquivo após sua gravação.

Os caracteres especiais "=" e "!" podem ser combinados em uma mesma regra.

Exemplo: Veja abaixo um exemplo de um arquivo `/etc/syslog.conf` padrão de sistemas `Debian`

```
#

# Primeiro alguns arquivos de log padrões. Registrados por facilidade

#

auth,authpriv.* /var/log/auth.log

*.*;auth,authpriv.none -/var/log/syslog

cron.* /var/log/cron.log

daemon.* -/var/log/daemon.log

kern.* -/var/log/kern.log

lpr.* -/var/log/lpr.log

mail.* /var/log/mail.log

user.* -/var/log/user.log

uucp.* -/var/log/uucp.log

#

# Registro de logs do sistema de mensagens. Divididos para facilitar

# a criação de scripts para manipular estes arquivos.
```

```
#
mail.info -/var/log/mail.info
mail.warn -/var/log/mail.warn
mail.err /var/log/mail.err
# Registro para o sistema de news INN
#
news.crit /var/log/news/news.crit
news.err /var/log/news/news.err
news.notice -/var/log/news/news.notice
#
# Alguns arquivos de registro "pega-tudo".
# São usadas "," para especificar mais de uma prioridade (por
# exemplo, "auth,authpriv.none") e ";" para especificar mais de uma
# facilidade.nível que será gravada naquele arquivo.
# Isto permite deixar as regras consideravelmente menores e mais legíveis
#
*.=debug;\
auth,authpriv.none;\
news.none;mail.none -/var/log/debug
*.=info;*.=notice;*.=warn;\
auth,authpriv.none;\
cron,daemon.none;\
mail,news.none -/var/log/messages
#
# Emergências são enviadas para qualquer um que estiver logado no sistema. Isto
# é feito através da especificação do "*" como destino das mensagens e são
```

```
# enviadas através do comando wall.
#
*.emerg *
#
# Eu gosto de ter mensagens mostradas no console, mas somente em consoles que
# não utilizo.
#
#daemon,mail.*;\
# news.=crit;news.=err;news.=notice;\
# *.=debug;*.=info;\
# *.=notice;*.=warn /dev/tty8
# O pipe /dev/xconsole é usado pelo utilitário "xconsole". Para usa-lo,
# você deve executar o "xconsole" com a opção "-file":
#
# $ xconsole -file /dev/xconsole [...]
#
# NOTA: ajuste as regras abaixo, ou ficará maluco se tiver um um site
# muito movimentado...
#
daemon.*;mail.*;\
news.crit;news.err;news.notice;\
*.=debug;*.=info;\
*.=notice;*.=warn |/dev/xconsole
# A linha baixo envia mensagens importantes para o console em que
# estamos trabalhando logados (principalmente para quem gosta de ter
# controle total sobre o que está acontecendo com seu sistema).
```

```
*.err;kern.debug;auth.notice;mail.crit /dev/console
```

17.2.2 klogd

Este daemon controla o registro de mensagens do kernel. Ele monitora as mensagens do kernel e as envia para o daemon de monitoramento `syslogd`, por padrão.

`klogd [`*`opções`*`]`

opções

-d

Ativa o modo de depuração do daemon

-f [arquivo]

Envia as mensagens do kernel para o arquivo especificado ao invés de enviar ao daemon do `syslog`

-i

Envia um sinal para o daemon recarregar os símbolos de módulos do kernel.

-I

Envia um sinal para o daemon recarregar os símbolos estáticos e de módulos do kernel.

-n

Evita a operação em segundo plano. Útil se iniciado pelo `init`

-k [arquivo]

Especifica o arquivo que contém os símbolos do kernel. Exemplos deste arquivo estão localizados em `/boot/System.map-xx.xx.xx`.

A especificação de um arquivo com a opção `-k` é necessária se desejar que sejam mostradas a tabela de símbolos ao invés de endereços numéricos do kernel.

17.3 logger

Este comando permite enviar uma mensagem nos log do sistema. A mensagem é enviada aos logs via daemon `syslogd` ou via soquete do sistema, é possível especificar a prioridade, nível, um nome identificando o processo, etc. Seu uso é muito útil em shell scripts ou em outros eventos do sistema.

`logger [`*`opções`*`] [`*`mensagem`*`]`

Onde:

mensagem

Mensagem que será enviada ao daemon *syslog*

opções

-i

Registra o PID do processo

-s

Envia a mensagem ambos para a saída padrão (STDOUT) e syslog.

-f [arquivo]

Envia o conteúdo do arquivo especificado como *mensagem* ao syslog.

-t [nome]

Especifica o nome do processo responsável pelo log que será exibido antes do PID na mensagem do syslog.

-p [prioridade]

Especifica a prioridade da mensagem do syslog, especificada como `facilidade.nível`. Veja os tipos de prioridade/níveis em Arquivo de configuração`syslog.conf`, Seção 17.2.1.1. O valor padrão *prioridade.nível* é *user.notice*

Mais detalhes sobre o funcionamento sobre o daemon de log do sistema `syslogd`, pode ser encontrado em syslogd, Seção 17.2.1

Exemplos: `logger -i -t focalinux Teste teste teste`, `logger -i -f /tmp/mensagem -p security.emerg`