**Conhecendo os arquivos de log do Ubuntu Linux**

Por [Felipe Arruda](http://canaltech.com.br/autor/Felipe-Arruda/) [RSS](http://canaltech.com.br/rss/autor/Felipe-Arruda/)



[Enviar por Email](mailto:?subject=Conhecendo%20os%20arquivos%20de%20log%20do%20Ubuntu%20Linux&body=http://canaltech.com.br/tutorial/linux/conhecendo-os-arquivos-de-log-do-ubuntu-linux/)

http://canalte.ch/SGOU

[inShare](javascript:void(0);)

Um arquivo de log armazena mensagens emitidas pelo sistema operacional e por programas em execução, tanto durante o funcionamento quanto em falhas que eles possam vir a ter. Como você pode imaginar, esse tipo de arquivo acaba se tornando uma ferramenta importante para administradores de sistemas, já que guarda o registro dos principais eventos da máquina.

Outra característica importante dos arquivos de log é que eles nunca são sobrescritos, ou seja, as mensagens novas são adicionadas ao fim do arquivo, mas não substituem as mais antigas. Por meio desse histórico dos logs é possível descobrir, por exemplo, o que causou a interrupção de um software em certa data e horário e, a partir disso, encontrar soluções.

Os arquivos de log são o primeiro local para onde devemos olhar quando alguma coisa estranha acontece, e cada linha deles possui informações muito condensadas, mas sempre úteis. Por exemplo:

*May 20 11:37:47 felipe-VirtualBox sudo: pam\_unix(sudo:session): session opened for user root by felipe(uid=0)*

Essa linha poderia ser interpretada da seguinte maneira: no dia 20 de maio, às 11h37, o usuário *felipe*, de UID 0, requisitou na máquina *felipe-VirtualBox* as permissões de superusuário (*root*) por meio do comando *sudo*.

Com essa informação em mãos, já sabemos por onde começar a investigação caso alguma falha inexplicável tenha acontecido em regiões mais protegidas do sistema, por volta desse horário.

**Os principais arquivos de log**

Como já descrito no tutorial "[Entendendo a estrutura de diretórios do Linux](http://corporate.canaltech.com.br/tutorial/linux/Entendendo-a-estrutura-de-diretorios-do-Linux/)", o diretório */var* contém arquivos que aumentam de tamanho ao longo do tempo. Portanto, nada mais justo do que os arquivos de log do sistema também ficarem aqui, mais especificamente em */var/log*.

E antes de entrarmos em detalhes sobre como lidar com eles, vamos conhecer os principais arquivos de log do Ubntu. Vale a pena lembrar que os nomes e descrições desses logs também valem para outras distros Linux:

* **apt/** - diretório com logs de uso do gerenciador de pacotes [apt-get](http://canaltech.com.br/tutorial/linux/Ubuntu-Linux-gerenciando-pacotes-com-o-apt-get/);
* **boot.log** - registro dos serviços carregados durante a inicialização do sistema;
* **dmesg** - log do último boot;
* **lastlog** - arquivo binário com dados de logins e desligamentos, usados pelo comando *last*;
* **auth.log** - registro do uso de autorizações do sistema, como mecanismos que exigem senhas. Exemplo: o comando *sudo* ou logins SSH remotos;
* **daemon.log** - arquivo com registro sobre as atividades dos daemons, serviços executados em segundo plano;
* **debug** - mensagens do sistema e de aplicações em geral em modo de *debug*;
* **kern.log** - mensagens detalhadas do kernel do Ubuntu Linux;
* **syslog** - mensagens do Ubuntu Linux que não foram armazenadas em logs mais específicos. Consulte-o quando você não achar a mensagem desejada em outros arquivos;
* **Xorg.0.log** - informações sobre drivers da placa de vídeo e o ambiente gráfico.

Além desses, o */var/log* ainda contém subdiretórios usados por programas que separam as mensagens de log em vários arquivos, como apache, samba etc.

**Operações básicas com logs**

Para visualizar o conteúdo de um arquivo de log, basta usar o comando *less*, passando como parâmetro o caminho e nome do arquivo a ser visualizado. Lembre-se que você não precisa percorrer as inúmeras linhas de texto do arquivo para encontrar a entrada correta: basta pesquisar por uma palavra-chave.

Para isso, durante a execução do *less*, pressione a tecla da barra (*/*) e, em seguida, digite o termo desejado e pressione Enter. Para procurar por outras ocorrências da palavra pesquisada, pressione a tecla "n".

Caso deseje visualizar apenas as primeiras linhas de um arquivo de log, use o comando *head arquivo.log*. Você pode estipular o número de linhas a serem exibidas da seguinte forma: *less -n 20 arquivo.log*. Nesse caso, por exemplo, serão exibidas as 20 primeiras linhas do arquivo.

Já o fim do arquivo pode ser visto com o comando *tail*, que possui sintaxe bem semelhante à do head: *tail arquivo.log* ou, se preferir, *tail -n 2 arquivo.log*.

Porém, é provável que o parâmetro mais usado do tail seja o "-f", que permite visualizar em tempo real as alterações sofridas por um arquivo de log: *tail -f arquivo.log*. Com ele você poderá realizar testes e conferir, em tempo real, que tipo de mensagens os arquivos de log receberão. Para interromper o *tail -f*, basta usar a combinação de teclas Ctrl + C.

E já que logs, na maior parte das vezes, não passam de grandes arquivos de texto puro, nada como usar o *grep* para ajudar a localizar rapidamente as linhas mais importantes. Você pode pesquisar por um termo em um arquivo com a seguinte linha:

*grep palavra arquivo.log*

E também pode usar [expressões regulares](http://canaltech.com.br/tutorial/linux/Como-usar-expressoes-regulares-no-Linux/). Para procurar todas as linhas que começam com *system*, por exemplo, use:

*grep "^system" arquivo.log*

Caso o resultado seja longo demais para caber em uma tela, você pode redirecioná-lo para o comando *less*:

*grep "system" arquivo.log | less*

Em um próximo tutorial, exploraremos caaracterísticas mais avançadas dos sistemas de logs do Ubuntu Linux, incluindo detalhes de como forçar o sistema a enviar determinadas mensagens para um arquivo estipulado por você.

Este artigo faz parte de nossa biblioteca de conteúdo ["Tudo o que você precisa saber sobre o Linux"](http://canaltech.com.br/materia/linux/Biblioteca-de-conteudo-Tudo-o-que-voce-precisa-saber-sobre-Linux/). Não deixe de acessar e conferir todo o conteúdo publicado sobre o Pinguim.

Matéria completa: <http://canaltech.com.br/tutorial/linux/conhecendo-os-arquivos-de-log-do-ubuntu-linux/#ixzz3r30UmxFZ>   
O conteúdo do Canaltech é protegido sob a licença Creative Commons (CC BY-NC-ND). Você pode reproduzi-lo, desde que insira créditos COM O LINK para o conteúdo original e não faça uso comercial de nossa produção.