

# Sessão 5 — Registro de eventos



As atividades 1, 2 e 3 desta sessão serão realizadas na máquina virtual *Client\_Linux*. As atividades 4, 5, 6 e 7 serão realizadas em ambas as máquinas *Server\_Linux* e *Client\_Linux*, de acordo com o enunciado de cada exercício.



Em algumas atividades, você trabalhará com a conta **root**, o que lhe dará todos os direitos sobre os recursos do sistema. Seja cauteloso antes de executar qualquer comando.

## 1) Registrando os eventos do kernel

1. Configure seu sistema de modo que os eventos gerados pelo kernel sejam registrados em um arquivo chamado **kernel.log**, no diretório **/var/log**.

## 2) Analisando os arquivos de log do sistema

Para esta atividade você terá que ter acesso **ssh** à máquina em que está configurando o sistema de logs para que você possa acompanhar, em tempo real, os registros gravados nos arquivos de log.

1. Crie, em sua máquina, uma conta com senha para acesso via **ssh**.
2. A partir de uma máquina remota, faça login via **ssh** utilizando a conta criada no passo anterior. Utilize o comando **tail** com a opção **-f** para verificar em tempo real os registros gerados pelo **syslog** no arquivo **/var/log/auth.log**.
3. Faça um *script* que contabilize o número de tentativas de login mal sucedidas através do **ssh**, listando os IPs de origem e quantas tentativas foram feitas por cada IP.

## 3) Analisando os arquivos de log binários do sistema

Nesta atividade, você irá trabalhar com os arquivos de log binários armazenados no diretório **/var/log**.

1. Verifique quais foram os dois últimos usuários a efetuarem login em seu computador.
2. Como você poderia verificar as contas existentes em seu computador que nunca efetuaram login?
3. Qual a maneira mais fácil de identificar um login remoto efetuado em seu computador?
4. Faça um *script* que mostre o tempo total que cada usuário ficou logado no sistema utilizando as informações obtidas com o comando **last**.

## 4) Servidor de log remoto

1. Este exercício deve ser feito utilizando duas máquinas virtuais Linux. Configure um servidor de logs na máquina virtual *Server\_Linux*; posteriormente, configure a máquina virtual *Client\_Linux* para enviar os registros dos eventos gerados para esse servidor de logs.

2. Após terminar a configuração, efetue um login na máquina *Client\_Linux* em um terminal qualquer e verifique onde foi registrado esse evento no servidor de logs *Server\_Linux*.
3. Cite três vantagens obtidas com o uso de um servidor de logs.

## 5) Utilizando o logger

Nesta atividade, você irá verificar uma funcionalidade importante do comando `logger`.

1. Na máquina *Server\_Linux*, inclua uma nova regra no arquivo `/etc/rsyslog.conf`, de modo que qualquer evento gerado pelo daemon `cron` seja registrado no arquivo `/var/log/cron.log`.
2. Utilize o comando `logger` para testar se a alteração feita no passo anterior produziu o efeito esperado.

## 6) Rotacionando arquivos de log do sistema

Nesta atividade, você irá configurar o rotacionamento dos arquivos de log de seu computador.

1. Na máquina *Server\_Linux*, realize o rotacionamento mensal do arquivo recém-criado `/var/log/cron.log`, mantendo uma cópia dos dois últimos arquivos compactados e criando, automaticamente, um novo arquivo vazio após o rotacionamento.

## 7) Aplicativos para análise de arquivos de log

1. Na máquina *Server\_Linux*, instale o pacote `logwatch` através do comando `apt-get` e configure-o para enviar um relatório diário do sistema para o usuário `root`. Um exemplo do arquivo de configuração está disponível em `/usr/share/logwatch/default.conf/logwatch.conf`.
2. Ainda na máquina *Server\_Linux*, crie uma regra para o `swatch` que envie um e-mail de notificação ao administrador quando alguma tentativa de login via `ssh`, ou `su` para o usuário `root`, falharem.
3. Ainda na máquina *Server\_Linux*, habilite o `logcheck` para enviar relatórios ao usuário `root` de 30 em 30 minutos (ex: 1:00, 1:30, etc.).

## 8) Recomendações básicas de segurança

1. O que você faria para aumentar o nível de segurança em um servidor de logs centralizado? Cite duas opções.