Sistemas de logs

Esta atividade visa dar uma visão mais profunda dos sistemas de coleta de eventos (*logs*) de dois sistemas UNIX e Windows típicos.

Logs em Linux

A coleta e gerência de logs em sistemas UNIX está a cargo de um subsistema específico, composto pelo *Syslog Daemon*, bibliotecas para geração de logs e alguns utilitários. Quase todas as versões recentes de distribuições Linux usam o RSyslog (*Reliable Syslog*), uma versão estendida e compatível do *syslog* tradicional.

Explorando logs

Os principais arquivos de logs do Linux estão armazenados no diretório `/var/log/`.

1. Identifique cada um dos arquivos presentes no diretório `/var/log/`.
2. Quais desses arquivos são gerados pelo *RSyslog* e quais são gerados por outros subsistemas?[1)]
3. Explique a estrutura de uma linha típica do arquivo `/var/log/syslog`.
4. O que representam os arquivos com nome `*.1.gz`, `*.2.gz`, etc.? (dica: `man logrotate`)

Configurando o subsistema de logs

Em uma máquina virtual, configure o subsistema de logs do Linux para atender os seguintes requisitos:

1. Eventos do subsistema de e-mail devem ir para o arquivo `/var/log/mail.log`.
2. Eventos de prioridade `emerg` ou superior devem ser registrados no arquivo `/var/log/emergency.log`, divulgados nos terminais de todos os usuários conectados e enviados a um servidor de logs externo (*logserver*) usando UDP.
3. Eventos de prioridade `crit` ou superior devem ser registrados no arquivo `/var/log/critical.log`, divulgados nos terminais do administrador e postados no Twitter (dica: escreva um script para executar o comando `tweet` do pacote *python-twitter*) ou no Telegram (http://www.bernaerts-nicolas.fr/linux/75-debian/351-debian-send-telegram-notification).

Para testar suas configurações, use o comando `logger`, que permite gerar mensagens de log a partir da linha de comando ou de scripts.

Logs em Windows

Sistemas Windows registram seus eventos de forma conceitualmente similar aos sistemas UNIX, embora suas implementações sejam muito diferentes. A ferramenta *Event Viewer*, disponível no painel de controle (em *Ferramentas Administrativas*), permite a visualização de logs.

As seguintes URLs contêm algumas informações adicionais sobre logs em sistemas Windows:

- https://docs.microsoft.com/en-us/windows/win32/wes/windows-event-log
- http://en.wikipedia.org/wiki/Event_Viewer

Explorando logs

Usando a ferramenta *Event Viewer*:

1. identifique os grandes domínios de logs gerados no sistema.
2. analise o conteúdo/significado de uma entrada típica em cada uma dessas áreas.
3. identifique os níveis de prioridade e categorias dos eventos gerados.

Gerando logs

1. Use o utilitário de linha de comando `eventcreate` para criar entradas de log fictícias, uma em cada domínio identificado acima, com prioridades e categorias diversas.

[1)]

Informação adicional pode ser obtida nos arquivos de configuração do RSyslog, em `/etc/rsyslog.*`.