Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Proceso de logs sencillo (12152 lectures)

Per **Mateu Batle Sastre**, ***Mateu*** (http://www.mbatle.com/)

Creado el 16/06/2001 11:56 modificado el 16/06/2001 11:56

Unos pequeños trucos para procesar logs muy fácilmente, sin necesidad de aprender awk o perl. Con unos sencillos comandos se puede extraer información muy valiosa de los logs del sistema.

Este artículo está pensado para principiantes en Linux.
Una lista de algunos comandos útiles para proceso de logs:

- **grep**: filtrado de lineas de ficheros. Saca sólo aquellas líneas que incluyen una determinada palabra o patrón (con expresiones regulares).
- **cut**: divide una línea en campos, permitiendo seleccionar uno o varios.
- **sort**: ordena alfabéticamente los resultados.
- **uniq**: elimina duplicados.
- **xargs**: aplica un comando sobre cada resultado.
- **host**: averiguar el nombre de host y dominio asociado a una IP.

El proceso es bastante simple, a partir de un fichero de log escogemos las líneas que nos interesan (grep) y los campos dentro de la línea(cut), posteriormente viene la parte de procesamiento de esta información. Ahora sólo queda juntar los comandos con pipes y listos. Vamos a ver unos ejemplos:

- **Ordenadores que han atacado a nuestro firewall:**

  Para esto será necesario que activemos la opción de logging en las ipchains, peró esto ya queda fuera del objetivo de este truco. El comando seria el siguiente:

```
grep Packet /var/log/messages | cut -f 12 -d ' ' | cut -f 1 -d ':' | sort
| uniq | xargs -n 1 host
```

- **Puertos TCP/UDP que han sufrido un ataque:**

```
grep Packet /var/log/messages | cut -f 13 -d ' ' | cut -f 2 -d ':' | sort
| uniq
```

- **Quien ha accedido a nuestro web:**

```
cut -f 1 -d ' ' /var/log/httpd/access_log | sort | uniq | xargs -n 1 host
```

Estos ejemplos han sido ejecutados en una distribución Red Hat 7.1 sin problemas. Es posible que en otras distribuciones los nombres de los logs sean diferentes o esten en diferentes formatos.

--Mateu

E-mail del autor: mbatle _ARROBA_ mbatle.com
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=675