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

Logear Netfilter en una base de datos (13866 lectures)

Per **Oriol Raventos**, ***w00g*** (http://www.oxhuge.com)

Creado el 17/10/2002 23:56 modificado el 17/10/2002 23:56

Cómo sabeis, Netfilter reemplazó a IPChains como sistema de filtrado de paquetes en Linux. Una de las novedades de Netfilter es el target ULOG que, junto al daemon ulogd, permite logear de forma mucho más flexible que la típica combinación LOG+syslog.

En este artículo explicaré cómo hacer que Netfilter logee a una base de datos MySQL.

Hace tiempo que quería tener el log de netfilter en una base de datos porque hacer consultas es mucho más potente que "grepear" logs, así que perpetré un invento[1] que cumplía con el cometido. Luego descubrí ULOG y recordé una lección muy valiosa: no te lanzes a hacer algo sin antes averiguar si ya está hecho ;P ..bueno, me dejo de rollos y vamos al grano.

Este artículo está orientado a Debian, pero hacer que funcione en otras distribuciones, cómo siempre, no será demasiado complicado. También se supone que no hemos instalado previamente MySQL en este host.

ajustando el kernel

con un kernel instalado desde un paquete oficial, puedes usar modconf para cargar los módulos de forma permanente.

sino, debes asegurarte de tener compilado el kernel con las opciones

```
CONFIG_NETFILTER
CONFIG_IP_NF_IPTABLES
CONFIG_IP_NF_FILTER
CONFIG_IP_NF_TARGET_ULOG
```

si usas menuconfig, hay que seleccionar

```
Networking options > Network packet filtering
Networking options > Netfilter Configuration > IP tables support
Networking options > Netfilter Configuration > Packet filtering
Networking options > Netfilter Configuration > ULOG target support
```

en función de tu configuración puede que necesites otras opciones relacionadas, suelen ser habituales las siguientes

```
CONFIG_IP_NF_CONNTRACK
CONFIG_IP_NF_FTP
CONFIG_IP_NF_IRC
```

ulogd

ulogd[2] es el daemon de logeo específico para el target ULOG así que deberemos instalarlo

```
apt-get install ulogd-mysql
```

Si estás usando un kernel 2.4.18 o superior en Woody o Sarge los paquetes oficiales no te funcionarán. Se puede leer el problema aquí[3], cómo ese era mi caso, hice unos paquetes nuevos que podéis descargar aquí (ulogd[4] y ulogd-mysql[5]) .. una vez descargados, los instalamos con

```
dpkg -i ulogd_0.97-1_i386.deb
dpkg -i ulogd-mysql_0.97-1_i386.deb
```

volveremos a ulogd luego

MySQL

como root, instalamos el servidor con

```
apt-get install mysql-server
```

al acabar, nos preguntará "should MySQL start on boot?", seleccionamos "Yes"

ahora ajustaremos MySQL, primero cambiamos el password del usuario root de MySQL (que no es el mismo que el root del sistema)

```
mysqladmin -u root password 'mi_password'
```

entramos

```
mysql -pmi_password
```

creamos la base de datos

```
mysql> create database logs;
Query OK, 1 row affected (0.02 sec)
```

creamos la tabla

```
mysql> use logs;
Database changed
mysql> source /usr/share/doc/ulogd-mysql/mysql.table
Query OK, 0 rows affected (0.00 sec)
```

creamos un par de usuarios y les damos los permisos necesarios

```
mysql> GRANT select,insert ON logs.* TO logwriter@localhost IDENTIFIED BY 'un_password';
Query OK, 0 rows affected (0.02 sec)
mysql> GRANT select ON logs.* TO logreader@localhost IDENTIFIED BY 'otro_password';
Query OK, 0 rows affected (0.02 sec)
mysql> flush privileges;
```

configuración de ulogd

abrimos /etc/ulogd.conf con un editor y quitamos los comentarios a las siguientes líneas

```
#mysqltable ulog
#mysqlpass bar
#mysqluser foo
#mysqldb ulogd
#mysqlhost localhost
#plugin /usr/lib/ulogd/ulogd_MYSQL.so
```

y ajustamos los parámetros necesarios

```
mysqluser logwriter
mysqlpass un_password
mysqldb logs
```

si no queremos que logee en un archivo de texto, podemos comentar las líneas

```
syslogfile /var/log/ulogd.syslogemu
plugin /usr/lib/ulogd/ulogd_LOGEMU.so
```

reiniciamos el servicio

```
/etc/init.d/ulogd restart
```

iptables

en nuestro script de iptables cambiamos todas las reglas con destino LOG por ULOG, lo podéis hacer a mano o con lo siguiente

```
perl -ne 's/-j\s+LOG/ULOG/i;print' -i scriptfw
```

os aconsejo que metáis una regla para comprobar que funciona, podría ser parecida a esta

```
iptables -A INPUT -i eth1 -s 192.168.100.0/24 -p tcp --dport 9999 \
-j ULOG    --log-prefix "test"
```

que luego probáis, por ejemplo, con hping

```
hping ip_interna_de_mi_cortafuegos -S -p 9999 -c 1
```

accediendo a los datos

afortunadamente se puede acceder MySQL desde prácticamente cualquier lenguaje de programación lo que hace realmente sencillo hacernos nuestras propias utilidades para hacer consultas sobre los datos. De todas formas, he encontrado un par de scripts php que pueden serviros ulogd-php[6] y ulog[7].

Lista de enlaces de este artículo:

1. http://www.oxhuge.com/bulma/articles/ulogd/nflog2db
2. http://www.gnumonks.org/projects/ulogd
3. http://lists.gnumonks.org/pipermail/ulogd/2002-October/000178.html
4. http://www.oxhuge.com/bulma/articles/ulogd/ulogd_0.97-1_i386.deb
5. http://www.oxhuge.com/bulma/articles/ulogd/ulogd-mysql_0.97-1_i386.deb
6. http://home.regit.org/ulogd-php.html
7. http://www.signuts.net/projects/id/42

E-mail del autor: oriol _ARROBA_ oxhuge.com