rsyslog

Rsyslog

En la instalación del servidor remoto de log’s se han usado las siguientes herramientas.

- CentOS 5.2
- Rsyslog
- Mysql
- PHP
- Apache
- Phplogcon

Instalación

Desde la consola introducimos lo siguiente:

yum –y install rsyslog rsyslog-mysql mysql-server php httpd php-mysql

Se instalarán automáticamente los paquetes arriba mencionados (menos el phplogcon) y además todas sus dependencias.

Configuración

Añadimos al sistema el usuario syslog que lo usaremos en la base de datos. # useradd syslog

Empezamos por arrancar y configurar el mysql.

chkconfig mysqld on

service mysqld start

Añadimos una clave para el root del mysql.

mysqladmin –u root password nueva-clave

rsyslog-mysql trae preparada una base de datos llamada syslog para crearla en mysql y meter ahí los datos que obtenemos. Para crearla hacemos lo siguiente:

cd /usr/share/doc/rsyslog-mysql-2.0.0 # mysql –p < createDB.sql

Una vez creada la base de datos nos logeamos como root en mysql y le damos permiso al usuario syslog para que pueda escribir en la base de datos.

mysql –u root –p mysql> grant all on Syslog.* to syslog@localhost identified by ‘syslogpwd’; mysql> flush privileges; mysql> exit

Ahora tenemos que modificar los dos ficheros de configuración del rsyslog.

/etc/rsyslog.conf → ejemplo para este fichero:

Log all kernel messages to the console. # Módulos para la comunicación con la base de datos en mysql $ModLoad ommysql.so $ModLoad imudp.so $UDPServerRun 514 . :ommysql:127.0.0.1,Syslog,syslog,syslogpwd # Logging much else clutters up the screen. #kern.* /dev/console # Log anything (except mail) of level info or higher. # Don't log private authentication messages! *.info;mail.none;authpriv.none;cron.none /var/log/messages # The authpriv file has restricted access. authpriv.* /var/log/secure # Log all the mail messages in one place. mail.* -/var/log/maillog # Log cron stuff cron.* /var/log/cron # Everybody gets emergency messages *.emerg * # Save news errors of level crit and higher in a special file. uucp,news.crit /var/log/spooler # Save boot messages also to boot.log local7.* /var/log/boot.log

/etc/sysconfig/rsyslog à ejemplo para este fichero:

Options to syslogd # -m 0 disables 'MARK' messages. # -rPortNumber Enables logging from remote machines. The listener will
listen
to the specified port. # -x disables DNS lookups on messages recieved with -r # See syslogd(8) for more details SYSLOGD_OPTIONS="-r -t514 -m 0" # Options to klogd # -2 prints all kernel oops messages twice; once for klogd to decode, and # once for processing with 'ksymoops' # -x disables all klogd processing of oops messages entirely # See klogd(8) for more details KLOGD_OPTIONS="-x"

El CentOS trae por defecto el syslog instalado para generar los log's, así que antes de arrancar el rsyslog tenemos que parar y deshabilitar el syslog para que no de problemas.

service syslog stop # chkconfig syslog off

service rsyslog start # chkconfig rsyslog on

También arracamos el apache.

service httpd start # chkconfig httpd on

Ya tenemos el rsyslog funcionando y grabando los log's en el mysql.

Lo siguiente será instalar el phplogcon, un frontal web que nos permitirá tener acceso de una forma cómoda a esos log's. Vamos a instalar la version 2.4.0 ques es la última estable a fecha de hoy (enero 2009)

Lo descargamos en el directorio tmp.

cd /tmp # wget http://www.phplogcon.org/Downloads-req-getit-lid-36.phtml

Lo descomprimimos:

tar xvzf phplogcon-2.4.0.tar.gz

Creamos una carpeta dentro de var/www para alojarlo y lo copiamos alli:

mkdir /var/www/phplogcon # cp -R /tmp/phplogcon-2.4.0/* /var/www/phplogcon

Nos situamos ahora en la carpeta /var/www/phplogcon/contrib y copiamos el configure.sh a la carpeta /var/www/phplogcon/src y lo ejecutamos para que nos cree el config.php que nos hace falta.

cd /var/phplogcon/contrib # copy configure.sh /var/www/phplogcon/src # ./configure.sh

Reiniciamos el apache.

service httpd restart

Ahora nos vamos a un navegador e introducimos la siguiente dirección → http://nuestra_ip/phplogcon/src

Esto lanzará un asistente que nos guiará en la configuración del phplogcon.

FAQ

A vece son tantos lo eventos que la base de datos acaba llenando el disco. Para liberar espacio necesitamos borrar algunos logs para llo ejecutamos lo siguiente;

```
#mysql -u usuario -p
#mysql> use Syslog;
#mysql> DELETE FROM SystemEvents WHERE ReceivedAt < date_add(current_date,
interval -30 day)
#mysql> optimize table SystemEvents;
#mysql> exit
```

From:
https://wiki.intrusos.info/ - **LCWIKI**

Permanent link:
https://wiki.intrusos.info/doku.php?id=aplicaciones:servidor_de_logs

Last update: **182023/01/ 13:10**