Hướng dẫn cài đặt Rsyslog 5.7.x trên nền tảng CentOS 5.x

QuanTriMang - Trong bài hướng dẫn sau, chúng tôi sẽ trình bày một số bước cơ bản để cài đặt và cấu hình syslog server bằng cách sử dụng Rsyslog. Theo thông tin từ phía hãng, Rsyslog có khả năng cải thiện khả năng hỗ trợ syslogd, có thể được sử dụng như 1 phương án thay thế hoặc dự phòng. Bên cạnh đó, những tính năng nâng cao khá phù hợp với các tầng lớp doanh nghiệp, khả năng bảo mật mã hóa cũng khá đơn giản và dễ thiết lập, dù cho đối tượng người sử dụng có ít kinh nghiệm. Cụ thể, chúng ta sẽ cùng nhau kết hợp và cài đặt tất cả các tính năng của Rsyslog 5.7.2 trên nền tảng CentOS 5.5 server.

Để bắt đầu, chúng ta cần cài đặt những gói hỗ trợ sau:

```
yum install -y pcre pcre-devel mysql-server mysql-devel gnutls gnutls-devel gnutls-utils net-snmp net-snmp-devel net-snmp-libs net-snmp-perl net-snmp-utils
```

```
libnet libnet-devel
```

Tiếp theo là gói *librelp (Reliable Event Logging Protocol Library)* để sử dụng các thư viện dành cho giao thức RELP – có nhiệm vụ cung cấp khả năng ghi lại các sự kiện xảy ra trong hệ thống mạng và đảm bảo rằng không bỏ sót bất kỳ tin nhắn cũng như email nào, cho dù có vấn đề xảy ra với quá trình kết nối hoặc các đầu peer không ổn định.

```
cd /tmp
wget
http://download.rsyslog.com/librelp/librel
p-1.0.0.tar.gz
tar -xvf librelp-1.0.0.tar.gz
cd librelp-1.0.0
./configure --prefix=/usr
make
make install
cd /tmp
wget
http://sourceforge.net/projects/libestr/fi
```

```
les/libestr-0.1.0.tar.gz/download
tar -xvf libestr-0.1.0.tar.gz
cd libestr-0.1.0
./configure --prefix=/usr
make
make install
cd /tmp
wget
http://www.libee.org/files/download/libee-
0.1.0.tar.gz
tar -xvf libee-0.1.0.tar.gz
cd libee-0.1.0
./configure --prefix=/usr
make
make install
```

Tại thời điểm bài viết này, chúng tôi sử dụng *rsyslog 5.7.2*:

```
cd /tmp
wget
```

```
http://www.rsyslog.com/files/download/rsyslog/rsyslog-5.7.2.tar.gz

tar -xvf rsyslog-5.7.2.tar.gz

cd rsyslog-5.7.2
```

Để tìm hiểu thông tin về những tùy chọn có sẵn trong Rsyslog, các bạn có thể sử dụng lệnh ***./configure –help***. Câu lệnh sau sẽ kích hoạt hầu hết các tính năng rsyslog như *Compression, Multithreading, MySql, SNMP, Mail, RELP... :*

```
./configure --enable-regexp --enable-zlib --enable-pthreads --enable-klog --enable-inet --enable-unlimited-select --enable-debug --enable-rtinst --enable-memcheck --enable-diagtools --enable-mysql --enable-snmp --enable-gnutls --enable-rsyslogrt --enable-rsyslogd --enable-extended-tests --enable-mail --enable-imptcp --enable-omruleset --enable-valgrind --enable-imdiag --enable-relp --enable-testbench --enable-imfile --enable-omstdout --enable-omdbalerting --enable-omuxsock --enable-
```

```
imtemplate --enable-omtemplate --enable-
pmlastmsg --enable-omudpspoof --enable-
omprog --enable-impstats

make

make install
```

Cài đặt và khởi tạo cơ sở dữ liệu MySQL:

```
mysql -u root -p <
plugins/ommysql/createDB.sql

mysql -u root -p mysql


GRANT ALL ON Syslog.* TO rsyslog@localhost
IDENTIFIED BY 'your-mysql-password';

flush privileges;
```

Tiếp theo, chúng ta sẽ cấu hình mã init:

```
vi /etc/init.d/rsyslog

#!/bin/bash

#

# rsyslog        Starts rsyslogd/rklogd.
```

```
#
#
# chkconfig: - 12 88
# description: Syslog is the facility by
which many daemons use to log \
# messages to various system log files.
It is a good idea to always \
# run rsyslog.
### BEGIN INIT INFO
# Provides: $syslog
# Required-Start: $local_fs $network
$remote_fs
# Required-Stop: $local_fs $network
$remote_fs
# Default-Stop: 0 1 2 3 4 5 6
# Short-Description: Enhanced system
logging and kernel message trapping
daemons
```

```
# Description: Rsyslog is an enhanced
multi-threaded syslogd supporting,
#              among others, MySQL,
syslog/tcp, RFC 3195, permitted
#              sender lists, filtering on
any message part, and fine
#              grain output format
control.
### END INIT INFO
# Source function library.
. /etc/init.d/functions
RETVAL=0
start() {
        [ -x /usr/local/sbin/rsyslogd ] ||
exit 5
        #[ -x /usr/local/sbin/rklogd ] ||
exit 5
        # Do not start rsyslog when
```

```
sysklogd is running
        if [ -e /var/run/syslogd.pid ] ;
then
                echo $"Shut down sysklogd
before you run rsyslog";
                exit 1;
        fi
        # Source config
        if [ -f /etc/sysconfig/rsyslog ] ;
then
                . /etc/sysconfig/rsyslog
        else
                #SYSLOGD_OPTIONS="-c3"
                SYSLOGD_OPTIONS="-c5"
                #KLOGD_OPTIONS="-2"
        fi
        if [ -z "$SYSLOG_UMASK" ] ; then
              SYSLOG_UMASK=077;
```

```
        fi
        umask $SYSLOG_UMASK
        echo -n $"Starting system logger:
"
        daemon /usr/local/sbin/rsyslogd
$SYSLOGD_OPTIONS
        RETVAL=$?
        echo
        #echo -n $"Starting kernel logger:
"
        #daemon rklogd $KLOGD_OPTIONS
        #echo
        [ $RETVAL -eq 0 ] && touch
/var/lock/subsys/rsyslog
        return $RETVAL
}
stop() {
        #echo -n $"Shutting down kernel
```

```
logger: "
        #killproc rklogd
        #echo
        echo -n $"Shutting down system
logger: "
        killproc rsyslogd
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && rm -f
/var/lock/subsys/rsyslog
        return $RETVAL
}
reload()  {
    RETVAL=1
    syslog=`cat /var/run/rsyslogd.pid
2>/dev/null`
    echo -n "Reloading system logger..."
    if [ -n "${syslog}" ] && [ -e
```