Subject: Re: syslog not working in VPS
Posted by jvegaseg on Wed, 23 Jun 2010 20:02:08 GMT
View Forum Message <> Reply to Message

Dear Konstantin, thanks for your answer. As I said before:

1.- Services klogd and syslogd are running:

```
[root@dialer init.d]# service syslog status
syslogd (pid  30275) is running...
klogd (pid  30278) is running...
```

2.- Service syslog starts when machine starts and /etc/init.d/syslog seams to be the same as you called "unhacked":

```
#!/bin/bash
#
# syslog        Starts syslogd/klogd.
#
#
# chkconfig: 2345 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 syslog.
### BEGIN INIT INFO
# Provides: $syslog
### END INIT INFO

# Source function library.
. /etc/init.d/functions

RETVAL=0

start() {
        [ -x /sbin/syslogd ] || exit 5
        [ -x /sbin/klogd ] || exit 5

        # Source config
        if [ -f /etc/sysconfig/syslog ] ; then
                . /etc/sysconfig/syslog
        else
                SYSLOGD_OPTIONS="-m 0"
                KLOGD_OPTIONS="-2"
        fi

        if [ -z "$SYSLOG_UMASK" ] ; then
             SYSLOG_UMASK=077;
        fi
```

```
        umask $SYSLOG_UMASK

        echo -n $"Starting system logger: "
        daemon syslogd $SYSLOGD_OPTIONS
        RETVAL=$?
        echo
        echo -n $"Starting kernel logger: "
        daemon klogd $KLOGD_OPTIONS
        echo
        [ $RETVAL -eq 0 ] && touch /var/lock/subsys/syslog
        return $RETVAL
}
stop() {
        echo -n $"Shutting down kernel logger: "
        killproc klogd
        echo
        echo -n $"Shutting down system logger: "
        killproc syslogd
        RETVAL=$?
        echo
        [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/syslog
        return $RETVAL
}
rhstatus() {
        status syslogd
        status klogd
}
restart() {
        stop
        start
}
reload()  {
    RETVAL=1
    syslog=`cat /var/run/syslogd.pid 2>/dev/null`
    echo -n "Reloading syslogd..."
    if [ -n "${syslog}" ] && [ -e /proc/"${syslog}" ]; then
        kill -HUP "$syslog";
        RETVAL=$?
    fi
    if [ $RETVAL -ne 0 ]; then
        failure
    else
        success
    fi
    echo
    RETVAL=1
    echo -n "Reloading klogd..."
    klog=`cat /var/run/klogd.pid 2>/dev/null`
```

```
    if [ -n "${klog}" ] && [ -e /proc/"${klog}" ]; then
        kill -USR2 "$klog";
        RETVAL=$?
    fi
    if [ $RETVAL -ne 0 ]; then
        failure
    else
        success
    fi
    echo
    return $RETVAL
}
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  status)
        rhstatus
        ;;
  restart)
        restart
        ;;
  reload)
        reload
        ;;
  condrestart)
        [ -f /var/lock/subsys/syslog ] && restart || :
        ;;
  *)
        echo $"Usage: $0 {start|stop|status|restart|condrestart}"
        exit 2
esac

exit $?
```

3.- Some processes write some information in /var/log/messages:

```
Jun 20 05:36:01 dialer syslogd 1.4.1: restart.
Jun 20 11:09:08 dialer rssh[4059]: setting log facility to LOG_USER
Jun 20 11:09:08 dialer rssh[4059]: allowing scp to all users
Jun 20 11:09:08 dialer rssh[4059]: allowing sftp to all users
Jun 20 11:09:08 dialer rssh[4059]: setting umask to 022
Jun 20 11:09:08 dialer rssh[4059]: chrooting all users to /usr/local/chroot
Jun 20 11:09:08 dialer rssh[4059]: line 52: configuring user XXXX
```

Jun 20 11:09:08 dialer rssh[4059]: setting XXXX's umask to 022
Jun 20 11:09:08 dialer rssh[4059]: allowing scp to user XXXX
Jun 20 11:09:08 dialer rssh[4059]: allowing sftp to user XXXX
Jun 20 11:09:08 dialer rssh[4059]: chrooting XXXX to /usr/local/chroot
Jun 20 11:09:08 dialer rssh[4059]: chroot cmd line: /usr/local/libexec/rssh_chroot_helper 2 "/usr/libexec/openssh/sftp-server"

4.- dmesg command echoes nothing:

[root@dialer ~]# dmesg
[root@dialer ~]#

5.- Iptables is not logging in /var/log/messages. My iptables rules are:

iptables -A INPUT -j LOG --log-prefix '** IPTABLES **' --log-level 4
iptables -A OUTPUT -j LOG --log-prefix '** IPTABLES **' --log-level 4

Sumary:

a.- It is not a problem of not running the syslog service.
b.- It is a problem of the service itself or a problem of configuration

Please, could you give me any clue?

Thanks in advance