Subject: syslog not working in VPS
Posted by jvegaseg on Wed, 02 Jun 2010 09:16:21 GMT
View Forum Message <> Reply to Message

I have 3 VPS in with Centos 5.4 64 bits and uname -a reports: Linux develop 2.6.18-164.15.1.el5.028stab068.9 #1 SMP Tue Mar 30 18:07:38 MSD 2010 x86_64 x86_64 x86_64 GNU/Linux

The problems is that dmesg shows nothing in the 3 VPS's and some applications which were reporting in /var/log/messages are not reporting now.

I HN dmesg is working well.

Another issue with that is that 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
```

I was googleing a lot and I could not find any answer.

People could you help me?

Subject: Re: syslog not working in VPS
Posted by jvegaseg on Mon, 14 Jun 2010 20:12:48 GMT
View Forum Message <> Reply to Message

Could anyone help me???

Subject: Re: syslog not working in VPS
Posted by khorenko on Tue, 15 Jun 2010 07:13:25 GMT
View Forum Message <> Reply to Message

Hi,

i guess you have to configure and enable service "syslogd" inside a Container, it is disabled by default.

--
Konstantin

Subject: Re: syslog not working in VPS

Posted by jvegaseg on Tue, 15 Jun 2010 08:21:35 GMT

View Forum Message <> Reply to Message

syslogd is running:

```
[root@develop etc]# service syslog status
syslogd (pid  15479) is running...
klogd (pid  15500) is running...
[root@develop etc]#
```

And the config file is:

```
# Log all kernel messages to the console.
# 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
```

And syslog service starts when VPS stars.

Any clue?

Subject: Re: syslog not working in VPS

Posted by jvegaseg on Fri, 18 Jun 2010 07:11:41 GMT
View Forum Message <> Reply to Message

I upgraded to :

Linux dialer 2.6.18-194.3.1.el5.028stab069.6 #1 SMP Wed May 26 18:31:05 MSD 2010 x86_64 x86_64 x86_64 GNU/Linux

And the problem persist.

Could you saw my last replay?

Subject: Re: syslog not working in VPS
Posted by khorenko on Wed, 23 Jun 2010 14:34:30 GMT
View Forum Message <> Reply to Message

Hi,

you need to do several things in order to collect messages inside a Container:

1) install klogd. In my case it was a part of "sysklogd" package and was not installed by default.

```
[root@dhcp-10-30-19-35 run]# rpm -qf `which klogd`
sysklogd-1.4.1-46.el5
[root@dhcp-10-30-19-35 run]# cat /etc/*rele*
CentOS release 5.4 (Final)
```

2) "syslog" is hacked not to start klogd, so you need to revert the hack.

```
--- /etc/init.d/syslog.log      2010-06-23 18:22:06.000000000 +0400
+++ /etc/init.d/syslog  2010-06-23 18:22:39.000000000 +0400
@@ -38,14 +38,14 @@ start() {
        RETVAL=$?
        echo
        echo -n $"Starting kernel logger: "
-       passed klogd skipped #daemon klogd $KLOGD_OPTIONS
+        daemon klogd $KLOGD_OPTIONS
        echo
        [ $RETVAL -eq 0 ] && touch /var/lock/subsys/syslog
        return $RETVAL
 }
 stop() {
        echo -n $"Shutting down kernel logger: "
-       passed klogd skipped #killproc klogd
+        killproc klogd
        echo
        echo -n $"Shutting down system logger: "
        killproc syslogd
@@ -56,7 +56,7 @@ stop() {
 }
 rhstatus() {
        status syslogd
-       #status klogd
+        status klogd
 }
 restart() {
        stop
```

Why it was done so?:
it was done historically in order to maximize the performance: on the one hand you'd better run syslog because it collects a lot of logs from userspace applications, on the other hand messages from kernel most often are useless inside a Container.

Hope that helps.

--
Konstantin

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

Subject: Re: syslog not working in VPS
Posted by khorenko on Thu, 24 Jun 2010 11:54:46 GMT
View Forum Message <> Reply to Message

May be you have too low printk log levels?
Please, check sysctl "kernel.printk".
On my system it has value = "6   4   1   8"

--
Konstantin

Subject: Re: syslog not working in VPS
Posted by jvegaseg on Thu, 24 Jun 2010 15:20:17 GMT
View Forum Message <> Reply to Message

Dear Konstantin, thanks for your answer.

My system reports:

```
[root@dialer ~]# sysctl "kernel.printk"
kernel.printk = 6       4       1       7
```

If this were the problem, I have no idea how to change that values.

Subject: Re: syslog not working in VPS
Posted by Jean-Marc Pigeon on Fri, 25 Jun 2010 02:41:17 GMT
View Forum Message <> Reply to Message

Double check /etc/vz/vz.conf
make sure you have
IPTABLES="ipt_state ipt_conntrack ipt_LOG ipt_REJECT.....

Subject: Re: syslog not working in VPS
Posted by khorenko on Tue, 29 Jun 2010 10:03:20 GMT
View Forum Message <> Reply to Message

Ok,

in case there are no chances to get a look at the node, i suggest another way:
as i've checked and iptables logging works fine for me, i believe this is just some configuration issue.

So, can you please try to reproduce the issue on the clean node and write down all your actions?
i mean - from the very beginning: installing CentOS (which version, how was it installed - which packages, etc.), the process of OpenVZ installation, where did you take the template for your experimental Container, which commands you used to enabled iptables inside a CT, so everything.

After that i'll try to do the very same on my side.

Hope that helps.

--
Konstantin

Subject: Re: syslog not working in VPS
Posted by cmer on Tue, 29 Jun 2010 18:27:36 GMT

View Forum Message <> Reply to Message

Good morning.

I come to you because I met the same problem.

It is impossible to accommodate the packet drop on my VM and it is quite embarrassing.
For information the node happens to him though a house the packet DROP but not VM

Here is my file vz.conf iptables

IPTABLES="ipt_REDIRECT ipt_owner ipt_recent iptable_filter iptable_mangle ipt_limit ipt_multiport ipt_tos ipt_TOS ipt_REJECT ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_LOG ipt_length ip_conntrack ip_conntrack_ftp ip_conntrack_irc ipt_conntrack ipt_state ipt_helper iptable_nat ip_nat_ftp ip_nat_irc"

Is there a solution to the problem?

Subject: Re: syslog not working in VPS
Posted by jvegaseg on Wed, 30 Jun 2010 06:29:08 GMT

View Forum Message <> Reply to Message

In my vz.conf the iptables entry has the value of:

```
## IPv4 iptables kernel modules
IPTABLES="ipt_REJECT iptable_nat ipt_tos ipt_limit ipt_multiport iptable_filter iptable_mangle
ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length ipt_state ipt_LOG"
```

Subject: Re: syslog not working in VPS
Posted by cmer on Wed, 30 Jun 2010 20:45:36 GMT

View Forum Message <> Reply to Message

---

jvegaseg wrote on Wed, 30 June 2010 08:29In my vz.conf the iptables entry has the value of:

```
## IPv4 iptables kernel modules
IPTABLES="ipt_REJECT iptable_nat ipt_tos ipt_limit ipt_multiport iptable_filter iptable_mangle
ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length ipt_state ipt_LOG"
```

Hello.

Even with the rules that you have done this does not work: /

By cons when I type dmesg I may well appear in my iptables log VM

```
 dmesg
Firewall: *UDP_IN Blocked* IN=venet0 OUT= MAC= SRC=87.98.xxx.xxx DST=178.32.xx.xx
LEN=194 TOS=0x00 PREC=0x00 TTL=62 ID=0 DF PROTO=UDP SPT=28000 DPT=30001
LEN=174
Firewall: *TCP_IN Blocked* IN=venet0 OUT= MAC= SRC=193.107.xx.xx DST=178.32.xx.xx
LEN=60 TOS=0x00 PREC=0x00 TTL=53 ID=62566 DF PROTO=TCP SPT=59196 DPT=3306
WINDOW=5840 RES=0x00 SYN URGP=0
Firewall: *TCP_IN Blocked* IN=venet0 OUT= MAC= SRC=193.107.xx.xx DST=178.32.xx.xx
LEN=60 TOS=0x00 PREC=0x00 TTL=53 ID=62567 DF PROTO=TCP SPT=59196 DPT=3306
WINDOW=5840 RES=0x00 SYN URGP=0
Firewall: *TCP_IN Blocked* IN=venet0 OUT= MAC= SRC=193.107.xx.xx DST=178.32.xx.xx
LEN=60 TOS=0x00 PREC=0x00 TTL=53 ID=62568 DF PROTO=TCP SPT=59196 DPT=3306
WINDOW=5840 RES=0x00 SYN URGP=0
Firewall: *TCP_IN Blocked* IN=venet0 OUT= MAC= SRC=193.107.xx.xx DST=178.32.xx.xx
LEN=60 TOS=0x00 PREC=0x00 TTL=53 ID=62569 DF PROTO=TCP SPT=59196 DPT=3306
WINDOW=5840 RES=0x00 SYN URGP=0
Firewall: *TCP_IN Blocked* IN=venet0 OUT= MAC= SRC=193.107.xx.xx DST=178.32.xx.xx
LEN=60 TOS=0x00 PREC=0x00 TTL=53 ID=62570 DF PROTO=TCP SPT=59196 DPT=3306
WINDOW=5840 RES=0x00 SYN URGP=0
Firewall: *TCP_IN Blocked* IN=venet0 OUT= MAC= SRC=193.107.xx.xx DST=178.32.xx.xx
LEN=60 TOS=0x00 PREC=0x00 TTL=53 ID=62571 DF PROTO=TCP SPT=59196 DPT=3306
```

```
WINDOW=5840 RES=0x00 SYN URGP=0
Firewall: *UDP_IN Blocked* IN=venet0 OUT= MAC= SRC=87.98.xxx.xxx DST=178.32.xx.xx
LEN=199 TOS=0x00 PREC=0x00 TTL=62 ID=0 DF PROTO=UDP SPT=28001 DPT=30001
LEN=179
Firewall: *UDP_IN Blocked* IN=venet0 OUT= MAC= SRC=87.98.xxx.xxx DST=178.32.xx.xx
LEN=112 TOS=0x00 PREC=0x00 TTL=62 ID=0 DF PROTO=UDP SPT=28000 DPT=30001
LEN=92
```

But the log does not being written in the file /var/log/messages

---

Subject: Re: syslog not working in VPS
Posted by jvegaseg on Wed, 30 Jun 2010 21:30:47 GMT

View Forum Message <> Reply to Message

In my case, it does not work nor dmesg nor /var/log/messages.

Subject: Re: syslog not working in VPS
Posted by jvegaseg on Wed, 30 Jun 2010 21:41:09 GMT

View Forum Message <> Reply to Message

I will try to start from scratch but I have several VPS and it occurs the same in everyone.

If you think it is a configuration issue, what configurations should affect this issue?

I think there is a few "places" where configuration can affect.

Please, could you identify that "places" or configurations?

It could be only:

- It could be an IPTABLES configuration issue, but in this case, why dmesg is reporting nothing??
- It could be a syslog configuration issue, but in this case, why some applications are reporting well in /var/log/messages??

All of this has no much sense, it seems it could be simply a BUG. Syslog is disabled by default, so it could be not tested enough.
