
Subject: *SOLVED* APF not logging on openVZ VE
Posted by [ugob](#) on Fri, 18 May 2007 16:44:17 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hi,

I installed APF using this http://kb.swsoft.com/article_130_875_en.html article on different OpenVZ VEs and it cannot log at all. Not one iptables log entry in /var/log/messages.

However, I installed it on a simple host (no virtualization) and it logs perfectly. I don't see any errors in

May 18 12:02:05 server kernel: ** SSH ** IN=eth0 OUT=
MAC=00:30:bd:2c:f4:fb:00:50:7f:2f:76:fe:08:00 SRC=209.172.54.237 DST=10.1.1.10 LEN=60
TOS=0x00 PREC=0x00 TTL=53 ID=4390 DF PROTO=TCP SPT=54303 DPT=22
WINDOW=5840 RES=0x00 SYN URGP=0

Any idea?

Subject: Re: APF not logging on openVZ VE
Posted by [Vasily Tarasov](#) on Mon, 21 May 2007 06:30:46 GMT
[View Forum Message](#) <> [Reply to Message](#)

Are failcounters (/proc/user_beancounters) for VE in question clear?

Thanks

Subject: Re: APF not logging on openVZ VE
Posted by [ugob](#) on Tue, 22 May 2007 15:41:44 GMT
[View Forum Message](#) <> [Reply to Message](#)

Yes they ale....

101: kmemsize	2433162	3269484	92244787	101469265	0
lockedpages	0	0	4504	4504	0
privvmpages	18945	28959	154698	170167	0
shmpages	165	501	15469	15469	0
dummy	0	0	0	0	0
numproc	25	37	4000	4000	0
physpages	4101	5339	0	2147483647	0
vmguarpages	0	0	154698	2147483647	0
oomguarpages	4101	5339	154698	2147483647	0
numtcpsock	10	13	4000	4000	0
numflock	10	17	1000	1100	0
numpty	0	0	400	400	0

numsiginfo	0	3	1024	1024	0	
tcpsndbuf	105092	160764	14364262	30748262		0
tcprcvbuf	163840	283564	14364262	30748262		0
othersockbuf	44720	74488	7182131	23566131		0
dgramrcvbuf	0	4200	7182131	7182131		0
numothersock	34	47	4000	4000		0
dcachesize	0	0	20149933	20754432		0
numfile	1304	2156	36032	36032		0
dummy	0	0	0	0		0
dummy	0	0	0	0		0
dummy	0	0	0	0		0
numiptent	420	420	1000	1000		0

Subject: Re: APF not logging on openVZ VE
 Posted by [rickb](#) on Tue, 22 May 2007 22:12:58 GMT
[View Forum Message](#) <> [Reply to Message](#)

is syslog.conf the same on the VE and the server it works?

Subject: Re: APF not logging on openVZ VE
 Posted by [ugob](#) on Wed, 23 May 2007 02:03:54 GMT
[View Forum Message](#) <> [Reply to Message](#)

Relevant line:

On the VE

```
*.info;mail.none;authpriv.none;cron.none    -/var/log/messages
```

On the hardware server (works)

```
*.info;mail.none;authpriv.none;cron.none    /var/log/messages
```

However, I tried changing (removing the dash) and restarting syslog, still no logging for apf.

Subject: Re: APF not logging on openVZ VE
 Posted by [curx](#) on Wed, 23 May 2007 20:39:21 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hi,

is a kernel-logger started, like klogd ?
 Which OSTEMPATE is used ?

Subject: Re: APF not logging on openVZ VE
Posted by [ugob](#) on Thu, 24 May 2007 03:10:26 GMT
[View Forum Message](#) <> [Reply to Message](#)

Centos 4.

No, klogd is not running in the VE. None of my VE have klogd running, is that normal (all CentOS 4).

What should I do?

Thanks!

Subject: Re: APF not logging on openVZ VE
Posted by [ugob](#) on Fri, 01 Jun 2007 12:18:15 GMT
[View Forum Message](#) <> [Reply to Message](#)

Anyone has an answer? I'd like to have iptables logging in my VE, but klogd is not started...
Anyone got iptables to log in a VE?

Regards,

Ugo

Subject: Re: APF not logging on openVZ VE
Posted by [Vasily Tarasov](#) on Wed, 06 Jun 2007 11:52:08 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hello,

I've just found time to check ipt_LOG module in VE. It works for me, please, look at the transcript:

```
# lsmod | grep ipt_LOG
# modprobe ipt_LOG          # !!!! Loading ipt_LOG kernel module before VE start!
# lsmod | grep ipt_LOG
ipt_LOG          8192  0
x_tables        17928 13
ipt_LOG,xt_tcpudp,xt_state,xt_length,ipt_ttl,xt_tcpmss,ipt_TCPMSS,xt_multiport,xt_limit,ipt_tos,ipt
_REJECT,iptable_nat,ip_tables
# cat /etc/vz/conf/4.conf | grep ipt_LOG
# cat /etc/vz/vz.conf | grep ipt_LOG
```

```
# vim /etc/vz/vz.conf # !!!! Aadding ipt_LOG to the list of available in VE
# cat /etc/vz/vz.conf | grep ipt_LOG
IPTABLES="ipt_REJECT ipt_tos ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS
ipt_tcpmss ipt_ttl ipt_length ipt_state ipt_LOG"
# vzctl start 4
Starting VE ...
VE is mounted
Adding IP address(es): 10.0.1.2
Setting CPU units: 1000
Setting devices
File resolv.conf was modified
VE start in progress...
# vzctl enter 4
entered into VE 4
# dmesg
# iptables -A OUTPUT -j LOG
# echo $?
0
# ping mail.ru
PING mail.ru (194.67.57.126) 56(84) bytes of data.
64 bytes from mail.ru (194.67.57.126): icmp_seq=0 ttl=119 time=18.2 ms
64 bytes from mail.ru (194.67.57.126): icmp_seq=1 ttl=119 time=17.8 ms

--- mail.ru ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 17.815/18.056/18.297/0.241 ms, pipe 2
# dmesg
IN= OUT=venet0 SRC=10.0.1.2 DST=192.168.1.1 LEN=53 TOS=0x00 PREC=0x00 TTL=64
ID=59520 DF PROTO=UDP SPT=32768 DPT=53 LEN=33
IN= OUT=venet0 SRC=10.0.1.2 DST=194.67.57.126 LEN=84 TOS=0x00 PREC=0x00 TTL=64
ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=15423 SEQ=0
IN= OUT=venet0 SRC=10.0.1.2 DST=192.168.1.1 LEN=72 TOS=0x00 PREC=0x00 TTL=64
ID=59539 DF PROTO=UDP SPT=32768 DPT=53 LEN=52
IN= OUT=venet0 SRC=10.0.1.2 DST=194.67.57.126 LEN=84 TOS=0x00 PREC=0x00 TTL=64
ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=15423 SEQ=1
So, two important points:
1) Load ipt_LOG kernel module on VE0 _before_ VE start
2) Add ipt_LOG to the list of available modules in vz.conf
```

HTH,
Vasily

Subject: Re: APF not logging on openVZ VE
Posted by [ugob](#) on Thu, 19 Jul 2007 20:47:53 GMT
[View Forum Message](#) <> [Reply to Message](#)

Output of lsmod:

```
ip_tables          23568 14
iptables_nat,ipt_state,ipt_length,ipt_ttl,ipt_tcpmss,ipt_TCPMSS,iptable_mangle,ipt_multiport,ipt_limit,ipt_LOG,ipt_TOS,ipt_tos,ipt_REJECT,iptable_filter
```

Relevant line in /etc/sysconfig/iptables-config:

```
IPTABLES_MODULES="ipt_REJECT ipt_tos ipt_TOS ipt_LOG ip_conntrack ipt_limit ipt_multiport
iptables_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length ipt_state iptable_nat
ip_nat_ftp"
```

Now I restart the VE, and check /var/log/messages.

I tried connecting to a forbidden port, no log.