Subject: Logging from iptables died on latest kernel
Posted by james4 on Thu, 11 Jun 2009 13:59:52 GMT
View Forum Message <> Reply to Message

Hi,

After recently upgrading the kernel using yum, I seem to be having a problem with the kernel logging iptables output. This happens on the hardware node, and all virtual servers.

Prior to the update, the logging worked fine on the main and virtual servers, now none of them log.

What I have found out so far:
On initial boot up, messages are logged briefly until about 30 seconds after the VZ containers have been loaded (or sometimes until I ssh to a container). Then the logging of messages is stopped completely on virtual and main server, and thus I can't use a firewall to dynamically block people.

If I do "service vz stop", then as soon as they are all stopped, logging on the main server into /var/log/messages resumes, until I do a "service vz start" at which point it stops again.

This only occurs on the new kernel:
vmlinuz-2.6.18-128.1.1.el5.028stab062.3PAE

If I reselect the old kernel, all the messaging works as normal:
vmlinuz-2.6.18-92.1.18.el5.028stab060.8PAE

Not sure if this is something I can fix with help or if we need a new kernel without this issue?

Any help would be greatly appreciated!

Thanks,
James

Subject: Re: Logging from iptables died on latest kernel
Posted by james4 on Thu, 11 Jun 2009 21:16:49 GMT
View Forum Message <> Reply to Message

Just a little update on this, the trigger seems to be any one of the virtual machines trying to log some IP tables input. For as long as none of them try to log IP tables, all is fine.

Once any VM tries to log, iptables logging on the HN stops too. (This happens with even with a single iptable entry to log.)

As previously mentioned reverting back to the previous kernel with no other changes fixes the issue, and all VM's + HN log fine.

Any thoughts?

Thanks!

Subject: Re: Logging from iptables died on latest kernel
Posted by khorenko on Fri, 12 Jun 2009 09:15:27 GMT

View Forum Message <> Reply to Message

Hi James,

can you please write down a reproducer configuration?
i mean - how exactly did you configure Hardware Node and a Container in order they do iptables logging?

Thank you.

--
Konstantin

Subject: Re: Logging from iptables died on latest kernel
Posted by james4 on Fri, 12 Jun 2009 21:17:36 GMT

View Forum Message <> Reply to Message

I have managed to reproduce this error on a fresh install with different hardware. (Original was a web server running centos that I installed openvz on. Latest test was an install of centos under vmware workstation)

I've also made a copy of this post on bugzilla - http://bugzilla.openvz.org/show_bug.cgi?id=1284

Procedure that I have just done to replicate the problem:

I installed CentOS 5.2, because when I tried CentOS 5.3 I didn't know how to successfully downgrade the kernel for testing back and forth.

I then updated the kernel, kernel-devel and ovzkernel with yum, which gave me the option for the two kernel versions mentioned above which I can swap around using grub.

If anyone notices that I'm using a very out of date method here that could be the cause, please do let me know!

For HN

On the HN as reccomended to allow pass through:

```
iptables -A INPUT -i venet0 -j ACCEPT
iptables -A OUTPUT -o venet0 -j ACCEPT
iptables -A FORWARD -j ACCEPT -p all -s 0/0 -i venet0
iptables -A FORWARD -j ACCEPT -p all -s 0/0 -o venet0
```

On the HN as a basic firewall to allow ssh and block/log all else

```
iptables -A INPUT -d 192.168.2.161 -p tcp --dport 22 -j ACCEPT
iptables -P OUTPUT ACCEPT
iptables -A INPUT -d 192.168.2.161 -j LOG
iptables -A INPUT -d 192.168.2.161 -j DROP
```

Edit of vz.conf: (/etc/vz/vz.conf)

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

For Container

Downloaded
 http://download.openvz.org/template/precreated/centos-5-x86. tar.gz

Install from template - vzctl create 102 --ostemplate centos-5-x86
Set IP - vzctl set 102 --ipadd 192.168.2.162 --save
Set NS - vzctl set 102 --nameserver 192.168.2.1 --save

Then start container - service vz start - vzctl start 102

Setup similar basic logging firewall

```
iptables -A INPUT -d 192.168.2.162 -p tcp --dport 22 -j ACCEPT
iptables -P OUTPUT ACCEPT
iptables -A INPUT -d 192.168.2.162 -j LOG
iptables -A INPUT -d 192.168.2.162 -j DROP
```

Testing Process

On both HN and Container:

```
cd /var/log
tail -f messages
```

From another machine, telnet HN (any blocked/logged port)
Then repeat for container: telnet container (any blocked/logged port)

With older kernel, logs are sent to the appropriate place. IE on the HN it logs up blocked attempts directed at the HN, and the container logs are sent to the messages file within the container.

With the newer kernel, logs are sent to the HN until any attempt is made to log to the container, at which point all logging to both stops.

Subject: Re: Logging from iptables died on latest kernel
Posted by khorenko on Sat, 13 Jun 2009 06:03:26 GMT
View Forum Message <> Reply to Message

Great. Thank you very much for the reproducer, we'll have a look at it.