Subject: new centos update broke iptables
Posted by disco on Sun, 27 Apr 2014 12:40:58 GMT
View Forum Message <> Reply to Message

Hy,

with the recent update of the vzkernel to 2.6.32-042stab088.4 on centos 6.5 iptables's nat stopped working.

this is what I get when i try to start iptables

iptables: Setting chains to policy ACCEPT: filter [OK]
iptables: Flushing firewall rules: [OK]
iptables: Applying firewall rules: iptables-restore v1.4.7: iptables-restore: unable to initialize table 'nat'

Error occurred at line: 3
Try `iptables-restore -h' or 'iptables-restore --help' for more information.
[FAILED]

Subject: Re: new centos update broke iptables
Posted by Paparaciz on Mon, 28 Apr 2014 07:38:36 GMT
View Forum Message <> Reply to Message

just add iptable_nat to global or to CT config file.

as example:
IPTABLES="ipt_REJECT ipt_tos ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length iptable_nat"

after adding it you will need to restart vz service, and/or stop and start CT

Subject: Re: new centos update broke iptables
Posted by eega on Mon, 05 May 2014 19:05:18 GMT
View Forum Message <> Reply to Message

Its the same for me, however, it broke iptables on the host! How can I fix this?

Subject: Re: new centos update broke iptables
Posted by Paparaciz on Tue, 06 May 2014 07:04:07 GMT
View Forum Message <> Reply to Message

it seems there is 2 separate bugs there.

eega,
recent vzctl version disabled conntrack on ve0:

https://bugzilla.openvz.org/show_bug.cgi?id=2755

so you can change back setting:
echo 'options nf_conntrack ip_conntrack_disable_ve0=0' > /etc/modprobe.d/openvz.conf

reboot HN and should work ok.

for nat to work inside CT needs to be more investigated

Subject: Re: new centos update broke iptables
Posted by Paparaciz on Tue, 06 May 2014 07:44:31 GMT
View Forum Message <> Reply to Message

and after adding to iptable_nat to /etc/vz/vz.conf can't reproduce "disco" mentioned problem...

Subject: Re: new centos update broke iptables
Posted by eega on Tue, 06 May 2014 08:07:17 GMT
View Forum Message <> Reply to Message

Thank's, that fixed it!

Subject: Re: new centos update broke iptables
Posted by Grrruk on Wed, 07 May 2014 16:51:59 GMT
View Forum Message <> Reply to Message

Paparaciz, you saved me! It was incredibly difficult to find the solution. I have no NAT at all, but my iptables configuration a little bit hairy and suddenly hardware node became inaccessible after that update (VMs were ok, but it was impossible to log in to HN in any way). Fortunately I had iLO access to HN...

Subject: Re: new centos update broke iptables
Posted by ccto on Tue, 20 May 2014 07:06:34 GMT

ref.: http://kb.parallels.com/en/9630