Subject: BUG? OVZ 7 + CentOS 8 + iptables v1.8.4 (nf_tables)
Posted by andre on Thu, 09 Jul 2020 01:19:56 GMT
View Forum Message <> Reply to Message

It looks like as iptables is multiplying its rules at OVZ7+CentOS8

Steps bellow:

First, we confirm that there are no references to chain TEST

```
# iptables-save | grep -c TEST
# Warning: iptables-legacy tables present, use iptables-legacy-save to see them
0
```

Next, we create a chain TEST, a basic rule and at the end we count the number of references to it

```
# iptables -N TEST ; iptables -A TEST -j ACCEPT ; iptables-save | grep -c TEST
# Warning: iptables-legacy tables present, use iptables-legacy-save to see them
31
```

31 referentes. Shouldn't there be just 2? (chain creation + rule?)

Let's check which references are those:

```
# iptables-save
# Generated by iptables-save v1.8.4 on Wed Jul  8 22:11:17 2020
*filter
:INPUT ACCEPT [3859:241253]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [830:110277]
:TEST - [0:0]
-A TEST -j ACCEPT
-A TEST -j ACCEPT
-A TEST -j ACCEPT
-A TEST -j ACCEPT
COMMIT
# Completed on Wed Jul  8 22:11:17 2020
# Generated by iptables-save v1.8.4 on Wed Jul  8 22:11:17 2020
*raw
:PREROUTING ACCEPT [117105:12625485]
:OUTPUT ACCEPT [120335:94805945]
-A TEST -j ACCEPT
-A TEST -j ACCEPT
COMMIT
# Completed on Wed Jul  8 22:11:17 2020
```

```
# Generated by iptables-save v1.8.4 on Wed Jul  8 22:11:17 2020
*mangle
:PREROUTING ACCEPT [117100:12624568]
:INPUT ACCEPT [117100:12624568]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [120331:94804518]
:POSTROUTING ACCEPT [120331:94804518]
-A TEST -j ACCEPT
-A TEST -j ACCEPT
-A TEST -j ACCEPT
-A TEST -j ACCEPT
-A TEST -j ACCEPT
COMMIT
# Completed on Wed Jul  8 22:11:17 2020
# Generated by iptables-save v1.8.4 on Wed Jul  8 22:11:17 2020
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A TEST -j ACCEPT
-A TEST -j ACCEPT
-A TEST -j ACCEPT
-A TEST -j ACCEPT
COMMIT
# Completed on Wed Jul  8 22:11:17 2020
# Warning: iptables-legacy tables present, use iptables-legacy-save to see them
```

Subject: Re: BUG? OVZ 7 + CentOS 8 + iptables v1.8.4 (nf_tables)
Posted by vaverin on Thu, 09 Jul 2020 14:13:46 GMT
View Forum Message <> Reply to Message

Could you please specify kernel version is used on your node?
Also it's interesting how did you created Centos 8 container.
We saw some similar issue on old kernels,
it was fixed both in kernel and in centos 8 template settings (IIRC we have modified some config defaults).

thank you,
Vasily Averin

Subject: Re: BUG? OVZ 7 + CentOS 8 + iptables v1.8.4 (nf_tables)
Posted by andre on Thu, 16 Jul 2020 20:07:59 GMT
View Forum Message <> Reply to Message

Sorry for the delay, we redid all the steps with the lastest versions:
Kernel 3.10.0-1127.8.2.vz7.151.14
Virtuozzo Linux release 7.8.0 (627)

- created new template: yum install centos-8-x86_64-ez ; vzpkg create cache centos-8-x86_64
- created VE, started ve
- once inside VE:

systemctl disable firewalld ; systemctl stop firewalld
iptables-save | grep -c TEST
iptables -N TEST ; iptables -A TEST -j ACCEPT ; iptables-save | grep -c TEST

Result:

CT-105 /# iptables-save | grep -c TEST
1
CT-105 /# iptables -N TEST ; iptables -A TEST -j ACCEPT ; iptables-save | grep -c TEST
iptables: Chain already exists.
19
CT-105 /#

It looks like that the issue persists with the most recent version

Subject: Re: BUG? OVZ 7 + CentOS 8 + iptables v1.8.4 (nf_tables)
Posted by vaverin on Fri, 17 Jul 2020 05:50:01 GMT
View Forum Message <> Reply to Message

I've submitted
https://bugs.openvz.org/browse/OVZ-7223

Subject: Re: BUG? OVZ 7 + CentOS 8 + iptables v1.8.4 (nf_tables)
Posted by HHawk on Wed, 02 Dec 2020 13:14:30 GMT
View Forum Message <> Reply to Message

I am experiencing the same issue when setting up a new CT with CentOS 8.x along with DirectAdmin (CSF/LFD).
Exactly the same issues as mentioned by the topic starter.

Since this is already some time ago, I would assume it was fixed already, but apparently not?

When is this being fixed or even looked at?
...or is there a workaround?

Subject: Re: BUG? OVZ 7 + CentOS 8 + iptables v1.8.4 (nf_tables)
Posted by wsap on Thu, 03 Dec 2020 19:16:15 GMT
View Forum Message <> Reply to Message

Yep definitely seeing this issue here too. Had to convert a bunch of stuff to ipset to help lighten the overhead that this issue inevitably creates. Someone had commented in the official bug report that they didn't think this would be fixed until OpenVZ 8, but that seems pretty unlikely to me given that iptables management is handled by the OpenVZ kernel (ie: they have full access to deal with that) and even if the changes need to occur within the CentOS 8 container, that could be adjusted via the ez template.

Then again, devs have indeed taken their time with this...

Subject: Re: BUG? OVZ 7 + CentOS 8 + iptables v1.8.4 (nf_tables)
Posted by HHawk on Thu, 03 Dec 2020 20:07:43 GMT
View Forum Message <> Reply to Message

Yeah, exactly. I also emailed OpenVZ and Virtuozzo. And Virtuozzo responded quite quickly and logged in etc on the server I freshly created for their testing...
They appeared to be doing / testing stuff, but then they said I needed a Virtuozzo license. So I guess they don't really care even though OpenVZ 7 shares Virtuozzo 7 stuff.

Oh well. Maybe they will fix it. Hopefully sooner than later.

//edit

@Khorenko: maybe you can investigate this issue?

Subject: Re: BUG? OVZ 7 + CentOS 8 + iptables v1.8.4 (nf_tables)

Posted by HHawk on Wed, 09 Dec 2020 12:10:44 GMT
View Forum Message <> Reply to Message

Good news, after sending Virtuozzo (and OpenVZ) another email, I got a confirmation this issue and a fix will be applied in a future release.
I will quote their reply in here for everyone interested:

The case has been analyzed further, and submitted to the Development Team as internal issue with id #PSBM-105903; the issue will be investigated further on their side and the fix, once found, will considered to be included in one of the next product updates.

I am setting the status of this support ticket to "resolved" in recognition of the fact that Support Engineers have completed our portion of the work on this case.
Thank you for reporting an issue in our software.

So let's hope for a fix soon that we can use iptables without issues on e.g. CentOS 8.x + DirectAdmin.

Subject: Re: BUG? OVZ 7 + CentOS 8 + iptables v1.8.4 (nf_tables)
Posted by wsap on Fri, 02 Apr 2021 00:07:04 GMT
View Forum Message <> Reply to Message

While I'm grateful that they did fix these issues in the factory kernel, I'm a tad surprised that this didn't warrant the release of a new stable kernel after testing confirmed this bug was fixed.

This is currently one of the longest waits for a new stable kernel release. With vzkernel-3.10.0-1127.18.2.vz7.163.46.x86_64.rpm released on 20-Nov-2020 that makes over 4 months without security patches for OpenVZ users that don't have Virtuozzo licenses / ReadyKernel.