Subject: xt_NFQUEUE and netfilter_queue inside container not supported?
Posted by Lorddusty on Wed, 20 Oct 2010 17:52:34 GMT
View Forum Message <> Reply to Message

Hi,

for a filtering-applications I need xt_NFQUEUE available inside a container. The modules are properly loaded on hostnode and added to IPTABLES-Variable for this container.

But on starting the container I get

Unknown iptables-module xt_NFQUEUE: skipped
Unknown iptables-module netfilter_queue: skipped

This causes the application not to run as it can't connect to netfilter.

Does anyone have an idea how to solve this problem?

I'm running 2.6.27-openvz-levitan.1 on a gentoo-hostnode.

BR
Jens

Subject: Re: xt_NFQUEUE and netfilter_queue inside container not supported?
Posted by curx on Sat, 30 Oct 2010 16:50:00 GMT
View Forum Message <> Reply to Message

Hi,

after loading NFQUEUE is listed in: /proc/net/ip_tables_target

(ct0)-% vzctl exec <CTID> cat /proc/net/ip_tables_target

Bye,
Thorsten

Subject: Re: xt_NFQUEUE and netfilter_queue inside container not supported?
Posted by Lorddusty on Sat, 30 Oct 2010 21:04:16 GMT
View Forum Message <> Reply to Message

Hi,

well, I found out, that the target is available, but it is not possible to connect to nfqueue using

libnetfilter inside the container for processing those queued packets with userspace-application.

But the host-system is able to read and process containers queue. For now I set up a workaround running the application which decides how to handle a packet on the host-system. But for sure, this is only a dirty workaround.

As it works fine in 2.6.18-RHEL-Based kernel, this libnetfilter-connection hopefully will become available in 2.6.27/.32 or later somewhen soon.

BR
Jens

Subject: Re: xt_NFQUEUE and netfilter_queue inside container not supported?
Posted by curx on Sun, 31 Oct 2010 09:20:54 GMT
View Forum Message <> Reply to Message

Hi Jens,

please open a bug report to enable this feature in the development kernels at http://bugzilla.openvz.org/

Bye,
Thorsten

Subject: Re: xt_NFQUEUE and netfilter_queue inside container not supported?
Posted by Lorddusty on Sun, 31 Oct 2010 10:38:00 GMT
View Forum Message <> Reply to Message

Hi Thorsten,

this bug is already filed some days ago See Bug-ID 1677 (unfortunately I'm not allowed to post links yet

BR
Jens

Subject: Re: xt_NFQUEUE and netfilter_queue inside container not supported?
Posted by derbot on Tue, 22 Nov 2011 21:25:42 GMT
View Forum Message <> Reply to Message

hi,
has anyone succeded to use iptables NFQUEUE target inside VE ?
Bug-ID 1677 seems stalled.

Using:

2.6.26-2-openvz-686 (debian)

running the user-space program inside VE I'm getting:

strace:

```
bind(3, {sa_family=AF_NETLINK, pid=476, groups=00000000}, 12) = 0
write(1, "bind\n"..., 5bind
)               = 5
sendto(3, "\34\0\0\0\2\3\5\0\0\0\0\0\0\0\0\0\0\0\0\0\10\0\1\0\3\0\0\2"..., 28, 0,
{sa_family=AF_NETLINK, pid=0, groups=00000000}, 12) = -1 ECONNREFUSED (Connection
refused)
--- SIGSEGV (Segmentation fault) @ 0 (0) ---
+++ killed by SIGSEGV +++
```

running it in HN works as expected:

```
bind(3, {sa_family=AF_NETLINK, pid=16928, groups=00000000}, 12) = 0
write(1, "bind\n", 5bind
)                = 5
sendto(3, " \34\0\0\0\2\3\5\0\0\0\0\0\0\0\0\0\0\0\0\0\10\0\1\0\3\204\0\2 ", 28, 0,
{sa_family=AF_NETLINK, pid=0, groups=00000000}, 12) = 28
recvfrom(3, "$\0\0\0\2\0\0\0\0\0\0\0 B\0\0\0\0\0\0\34\0\0\0\2\3\5\0\0\0\0\0\0\0\0\0", 8192, 0,
{sa_family=AF_NETLINK, pid=0, groups=00000000}, [12]) = 36
```

Thanks,
Bogdan.

Subject: Re: xt_NFQUEUE and netfilter_queue inside container not supported?
Posted by spoke2u on Mon, 26 Jan 2015 03:04:20 GMT
View Forum Message <> Reply to Message

I recently been looking at this issue and I upgraded to latest kernel

uname -r
2.6.32-openvz-042stab102.9-amd64

vzctl --version
vzctl version 4.5.1

modprobe xt_mark
modprobe xt_conntrack
modprobe xt_NFQUEUE

modprobe xt_iprange

lsmod|grep -E "^x|^nf|^ip"|grep -Ev "^ip6|^ipv6|^nfs|^xhci"|sed "s| .*||"|sortiptable_filter
iptable_mangle
iptable_nat
ip_tables
ipt_LOG
ipt_REDIRECT
ipt_REJECT
nf_conntrack
nf_conntrack_ftp
nf_conntrack_ipv4
nf_defrag_ipv4
nf_nat
nf_nat_ftp
xt_dscp
xt_hl
xt_length
xt_limit
xt_multiport
xt_NFQUEUE
xt_state
xt_string
xt_TCPMSS
xt_tcpmss

I was able to run peerguardian then realized thats not what I really needed.

pglcmd start
[....] Starting PeerGuardian Linux: pgld.

hope this helps