Subject: Host-only network for CT [Vmware && Virtual Box style]
Posted by xdanx on Fri, 26 Aug 2011 22:12:39 GMT
View Forum Message <> Reply to Message

Hey everyone!

I started working with openVZ recently and I must admit it is awesome.
I have tested Xen Server, Vmware Server & ESXI , V-Server, VirtualBox and till now and OpenVZ seems to be exactly what I want.

Unfortunately, there is 1 problem to which I cannot find a solution:

Host-only network for CTs [Vmware , Virtual Box style]. I simply want to create a network with private IPs, where each container + the CT0 can talk to each other.

The only similar stuff I found on the internet are these:

www.shorewall.net/OpenVZ.html [it uses a bridge ?!]
forum.openvz.org/index.php?t=msg&goto=13255& [old post from 2007]

I managed to create a "mini" host-only network, only between 1 CT and the CT0 using the commands :

[host] vzctl set 100 --netif_add eth0
[host] ifconfig veth100.0 10.0.0.1 netmask 255.255.255.0
[host] vzctl enter 100
[CT] ifconfig eth0 10.0.0.10 netmask 255.255.255.0
[CT] route add default gw 10.0.0.1

And of course, with setup on the NAT on the host machine, it works.

I want this scenario because I would like to monitor the traffic to the CTs from the host [CT0] , and also setup DNAT [port forwarding].

Thank you for your time and hope this helps a bit,
Dan

Subject: Re: Host-only network for CT [Vmware && Virtual Box style]
Posted by kir on Mon, 29 Aug 2011 08:59:02 GMT
View Forum Message <> Reply to Message

Well there's no need to fiddle with veth in this setup. Use venet, it's easier.

Just assign an IP to each container using the private network (say 10.x.x.x), this way your containers will be able to talk to each other and the host system.

It's as simple as

vzctl set 101 --ipadd 10.11.12.101 --save

Subject: Re: Host-only network for CT [Vmware && Virtual Box style]
Posted by xdanx on Wed, 07 Sep 2011 23:20:25 GMT
View Forum Message <> Reply to Message

Ok, I created the network as you said.

vzctl set 101 --ipadd 10.0.2.10
vzctl set 102 --ipadd 10.0.2.11

So, the image is like this:

CT 1 : venet0:0 -> 10.0.2.10
CT 2 : venet0:0 -> 10.0.2.11
HN : NO IP in network 10.0.2.0/24 + eth0 -> 192.168.0.30

As you said, I can ping the CTs between them, I can ping from HN each CT , and I can ping from the CT the HN , on its eth0 address (192.168.0.30)

My questions are :

1) In order to fully create a host-only network, is it correct to add the HN the ip 10.0.2.1 :

[root@HN ~]# ifconfig venet0 10.0.2.1 netmask 255.255.255.0 ?

It is still a small problem, as the CTs can still ping 192.168.0.30 [the HN other IP] , which in a host-only network. Should I use iptables here ?

2) If I want to forward some ports from the HN to the CT nodes, what is the path the packets will take and what interfaces should I setup in the process ?
I was here wiki.openvz.org/Traffic_shaping_with_tc that the path packets take is

```
   venet0:0            venet0    eth0
CT >------------->-------------> HN >--------->--------> RH

   venet0:0            venet0    eth0
CT <-------------<-------------< HN <---------<--------< RH
```

3) On top of this thing I want to use SNORT to protect the CTs [all the open ports on the HN on the internet interface will be forwarded to the CTs] Where is better to put SNORT to listen ? on eth0 or venet0 on HN ?

Thanks and hope this will help anyone interested in creating host-only networks,
Dan
