
Subject: Networking, security

Posted by [andreas2](#) on Tue, 08 Sep 2009 14:55:50 GMT

[View Forum Message](#) <> [Reply to Message](#)

As I understood veth is a bridge, so all clients can listen to whole traffic.

Starting of /etc/init.d/libvirt-bin seems to be necessary to start dnsmasq, but can be stopped afterwards (starting "networking" clients after stopped works)

So what does libvirt do?

I've read it offers managing functions, so is it unsecure to have it running?

I would prefer to run few on the host, is it possible to give one vz-client the ability to manage other clients (so they would run inside this client)?

thanks, Andrew

Subject: Re: Networking, security

Posted by [kir](#) on Tue, 08 Sep 2009 16:24:27 GMT

[View Forum Message](#) <> [Reply to Message](#)

andreas2 wrote on Tue, 08 September 2009 18:55: As I understood veth is a bridge, so all clients can listen to whole traffic.

From vzctl man page:

`--mac_filter on|off`

Enables/disables MAC address filtering for the Container veth device and the possibility of configuring the MAC address of this device from inside the Container. If the filtering is turned on:

- * the veth device accepts only those packets that have a MAC address in their headers corresponding to that of this device (excluding all broadcast and multicast packets);

- * it is impossible to modify the veth MAC address from inside the Container.

By default, this functionality is enabled for all veth devices existing inside the Container.

Subject: Re: Networking, security

Posted by [kir](#) on Tue, 08 Sep 2009 16:29:13 GMT

[View Forum Message](#) <> [Reply to Message](#)

andreas2 wrote on Tue, 08 September 2009 18:55: Starting of /etc/init.d/libvirt-bin seems to be necessary to start dnsmasq

Neither libvirt nor dnsmasq is part of OpenVZ, so please address your question to their developers or your distro vendor.

PS1 sorry I do not understand the rest of your question

PS2 could you please follow the "one question-one topic" rule, otherwise it's not easy to answer and not convenient for the other users to read this afterwards.