Subject: several nics on the hn
Posted by Daniel Bauer on Thu, 06 Oct 2011 13:02:28 GMT
View Forum Message <> Reply to Message

Hello,

I've several nics on the hostnode. Only the internal service nic have an
internal IP. The other nics are without IPs and connected to different
internal subnets and public www.

I've read the differences between venet and veth
http://wiki.openvz.org/Differences_between_venet_and_veth
and want to use venet, but only venet0 is active in the hn, I think this
is connected to eth0, but how to access the other nics?

Thanks
Daniel

Subject: Re: several nics on the hn
Posted by Gary Wallis on Thu, 06 Oct 2011 13:24:54 GMT
View Forum Message <> Reply to Message

Edit your:

/etc/vz/vz.conf

Specifically the VE_ROUTE_SRC_DEV value

...
The name of the device whose IP address will be used as source IP for CT.
By default automatically assigned.
#VE_ROUTE_SRC_DEV="eth0"
...

Daniel Bauer wrote:
> Hello,
>
> I've several nics on the hostnode. Only the internal service nic have an
> internal IP. The other nics are without IPs and connected to different
> internal subnets and public www.
>
> I've read the differences between venet and veth
> http://wiki.openvz.org/Differences_between_venet_and_veth
> and want to use venet, but only venet0 is active in the hn, I think this
> is connected to eth0, but how to access the other nics?
>

> Thanks
> Daniel
>

Subject: Re: several nics on the hn
Posted by Gary Wallis on Thu, 06 Oct 2011 13:33:51 GMT
View Forum Message <> Reply to Message

If you need to have some containers use other NICs than the default, you
will need to probably to do some ip route stuff. Pretty advanced topic.
Of course you can always give container direct access to /dev devices
(like /dev/net/tun) via it's VEID.conf file. But that would involve all
kinds of very advanced routing and kernel expertise for sharing the
device among more than one container.

Subject: RE: several nics on the hn
Posted by Esm on Thu, 06 Oct 2011 13:55:02 GMT
View Forum Message <> Reply to Message

Hi Daniel,

What's your setup? You have 1 'internal' NIC with an IP-address and other
NIC's without IP-address who you want to connect inside a container, for
what purpose?

If you use veth you could theoretically set up a bridge with one of those
devices, that would be easiest in my opinion. But why would you consist on
venet?

Probably with a little bit more information we can help you a bit further.

Kind Regards,

Esmé

-----Oorspronkelijk bericht-----
Van: users-bounces@openvz.org [mailto:users-bounces@openvz.org] Namens
Daniel Bauer
Verzonden: donderdag 6 oktober 2011 15:02
Aan: users@openvz.org
Onderwerp: [Users] several nics on the hn

Hello,

I've several nics on the hostnode. Only the internal service nic have an

internal IP. The other nics are without IPs and connected to different
internal subnets and public www.

I've read the differences between venet and veth
http://wiki.openvz.org/Differences_between_venet_and_veth
and want to use venet, but only venet0 is active in the hn, I think this is
connected to eth0, but how to access the other nics?

Thanks
Daniel

Subject: RE: several nics on the hn
Posted by Esm on Thu, 06 Oct 2011 13:57:49 GMT
View Forum Message <> Reply to Message

"Routing stuff" is not more advanced then running an OpenVZ host with 5
containers and a firewall :)

-----Oorspronkelijk bericht-----
Van: users-bounces@openvz.org [mailto:users-bounces@openvz.org] Namens Gary
Wallis
Verzonden: donderdag 6 oktober 2011 15:34
Aan: users@openvz.org
Onderwerp: Re: [Users] several nics on the hn

If you need to have some containers use other NICs than the default, you
will need to probably to do some ip route stuff. Pretty advanced topic.
Of course you can always give container direct access to /dev devices (like
/dev/net/tun) via it's VEID.conf file. But that would involve all kinds of
very advanced routing and kernel expertise for sharing the device among more
than one container.

Subject: Re: several nics on the hn
Posted by Gary Wallis on Thu, 06 Oct 2011 14:56:16 GMT
View Forum Message <> Reply to Message

Esmé de Wolf wrote:
> "Routing stuff" is not more advanced then running an OpenVZ host with 5
> containers and a firewall :)
>
lol, yup ;)

But you got to admit that it is easy to mess up and not get what you
want when playing with tunnels, bridges and the ip command. Anybody can
follow the OpenVZ install instructions and have a working vz node with

50 containers in no time with no need to understand what is going on as long as everything is standard.

When you start mixing class Cs, venet, veth and what have you, is when you see forum postings.

Cheers,
Gary

Subject: Re: several nics on the hn
Posted by samiam on Thu, 06 Oct 2011 17:44:50 GMT
View Forum Message <> Reply to Message

> When you start mixing class Cs, venet, veth and what have you, is when you
> see forum postings.

I should note there is a RTFM on having different containers use different interfaces:

http://wiki.openvz.org/Source_based_routing

However, what is missing is a RTFM on having a single container use different interfaces to route to different IP ranges. For example, a host that is a router with separate interfaces to 192.168.1.0/24 and 192.168.42.0/24, as well as a gateway to the internet, and we want a container on this host to access all three networks (for example, a container running Squid as a web proxy).

Another example which has been annoying me: Having an OpenVZ container inside of a VirtualBox guest. I would like to have my OpenVZ container be accessible from both my host and access both the internet at the same time, in a way that does not require a bridged interface. [1] VirtualBox uses one interface to access the internet (10.0.4.X) and another interface that the host can use to connect to the guest (192.168.56.X). The OpenVZ container can connect to one or the other, but not both at the same time.

I just did a STFW to find a way to resolve this problem and only got other reports of people with similar issues, such as http://forum.openvz.org/index.php?t=msg&goto=9978&

So, here's my question: Is there a page out there which details exactly how to have an OpenVZ container use two or more different interfaces on the host machine?

- Sam

[1] The VirtualBox issue can be somewhat resolved by having the VirtualBox guest also have a bridged interface, and having the OpenVZ container use said bridged interface. This, alas, doesn't work when there isn't a DHCP server on the network to connect to, such as when I'm on a plane or somewhere else without WiFi.

Subject: Re: several nics on the hn
Posted by Daniel Bauer on Thu, 06 Oct 2011 20:13:50 GMT
View Forum Message <> Reply to Message

Hi Gary,

> If you need to have some containers use other NICs than the default,
> you will need to probably to do some ip route stuff. Pretty advanced
> topic. Of course you can always give container direct access to /dev
> devices (like /dev/net/tun) via it's VEID.conf file. But that would
> involve all kinds of very advanced routing and kernel expertise for
> sharing the device among more than one container.

The host node should only be accessible inside the service net, I don't want any routing or firewalling inside the hn, there should be no connection to the other nets like external.

Bye
Daniel

Subject: Re: several nics on the hn
Posted by Daniel Bauer on Thu, 06 Oct 2011 20:13:51 GMT
View Forum Message <> Reply to Message

Hi Esmé,

> What's your setup? You have 1 'internal' NIC with an IP-address and
> other
> NIC's without IP-address who you want to connect inside a container,
> for
> what purpose?

I've several nets:
1. internal service net, only available from/for the hostnode
2. internal LAN with intranet services for my users
3. DMZ
4. external IPs

The host node should only be accessible in net 1, I don't want any routing or firewalling inside the hn, there should be no connection f.e. to net 4

> If you use veth you could theoretically set up a bridge with one of
> those
> devices, that would be easiest in my opinion. But why would you
> consist on
> venet?

In the mentioned article the are two advantages: security and performance

> Probably with a little bit more information we can help you a bit
> further.

Thanks
Daniel

> -----Oorspronkelijk bericht-----
> Van: users-bounces@openvz.org [mailto:users-bounces@openvz.org] Namens
> Daniel Bauer
> Verzonden: donderdag 6 oktober 2011 15:02
> Aan: users@openvz.org
> Onderwerp: [Users] several nics on the hn
>
> Hello,
>
> I've several nics on the hostnode. Only the internal service nic have
> an
> internal IP. The other nics are without IPs and connected to different
> internal subnets and public www.
>
> I've read the differences between venet and veth
> http://wiki.openvz.org/Differences_between_venet_and_veth
> and want to use venet, but only venet0 is active in the hn, I think
> this is
> connected to eth0, but how to access the other nics?
>
> Thanks
> Daniel
>

Subject: Re: several nics on the hn
Posted by Daniel Bauer on Thu, 06 Oct 2011 20:19:47 GMT
View Forum Message <> Reply to Message

Hello Gary,

> Edit your:
>
> /etc/vz/vz.conf
>
> Specifically the VE_ROUTE_SRC_DEV value
>
> ...
> # The name of the device whose IP address will be used as source IP
> for CT.
> # By default automatically assigned.
> #VE_ROUTE_SRC_DEV="eth0"

I see that I could change this value, but not add an venet(1,2,3). I understand howto use veth, but then I loose the advantages of the venet ...

Thanks
Daniel

> Daniel Bauer wrote:
>> Hello,
>>
>> I've several nics on the hostnode. Only the internal service nic have
>> an
>> internal IP. The other nics are without IPs and connected to
>> different
>> internal subnets and public www.
>>
>> I've read the differences between venet and veth
>> http://wiki.openvz.org/Differences_between_venet_and_veth
>> and want to use venet, but only venet0 is active in the hn, I think
>> this
>> is connected to eth0, but how to access the other nics?
>>
>> Thanks
>> Daniel
>>

Subject: RE: several nics on the hn
Posted by Esm on Fri, 07 Oct 2011 08:23:00 GMT

Hey Daniel,

When you want to use this kind of configuration:

---internal---> | hn | VEID 1
---NIC 2----> | | VEID 2
---NIC 3----> | | VEID 3

And what you try is, f.e., to have the internal NIC only connecting to the hn, and NIC 2 to VEID 3 and NIC 3 to VEID 2, then you probably will need to route and firewall your config if you stick to venet.

Using a bridged setup would mean the same security implications as using the setup above (firewalled). So that's not something to worry about.

If you've any questions, please let us know.

Esmé

-----Oorspronkelijk bericht-----
Van: users-bounces@openvz.org [mailto:users-bounces@openvz.org] Namens Daniel Bauer
Verzonden: donderdag 6 oktober 2011 22:14
Aan: users@openvz.org
Onderwerp: Re: [Users] several nics on the hn

Hi Esmé,

> What's your setup? You have 1 'internal' NIC with an IP-address and
> other NIC's without IP-address who you want to connect inside a
> container, for what purpose?

I've several nets:
1. internal service net, only available from/for the hostnode 2. internal LAN with intranet services for my users 3. DMZ 4. external IPs

The host node should only be accessible in net 1, I don't want any routing or firewalling inside the hn, there should be no connection f.e. to net 4

> If you use veth you could theoretically set up a bridge with one of
> those
> devices, that would be easiest in my opinion. But why would you
> consist on
> venet?

In the mentioned article the are two advantages: security and
performance

> Probably with a little bit more information we can help you a bit
> further.

Thanks
Daniel

> -----Oorspronkelijk bericht-----
> Van: users-bounces@openvz.org [mailto:users-bounces@openvz.org] Namens
> Daniel Bauer
> Verzonden: donderdag 6 oktober 2011 15:02
> Aan: users@openvz.org
> Onderwerp: [Users] several nics on the hn
>
> Hello,
>
> I've several nics on the hostnode. Only the internal service nic have
> an
> internal IP. The other nics are without IPs and connected to different
> internal subnets and public www.
>
> I've read the differences between venet and veth
> http://wiki.openvz.org/Differences_between_venet_and_veth
> and want to use venet, but only venet0 is active in the hn, I think
> this is
> connected to eth0, but how to access the other nics?
>
> Thanks
> Daniel
>

Subject: Re: several nics on the hn
Posted by Benny Amorsen on Fri, 07 Oct 2011 10:00:45 GMT
View Forum Message <> Reply to Message

"Daniel Bauer" <mlist@dsb-gmbh.de> writes:

> Hello,
>
> I've several nics on the hostnode. Only the internal service nic have an
> internal IP. The other nics are without IPs and connected to different
> internal subnets and public www.

>
> I've read the differences between venet and veth
> http://wiki.openvz.org/Differences_between_venet_and_veth
> and want to use venet, but only venet0 is active in the hn, I think this
> is connected to eth0, but how to access the other nics?

What we do is a bit simpler: Just add the appropriate NIC into the
guest. This way the host loses access to the NIC and the guest can be
configured in exactly the same way a non-virtualized server would be
configured. Routing and firewalling is then done by our usual routers
and firewalls, again exactly like it works for non-virtualized servers.

To avoid having to put 50 NIC's in each VZ server we actually do it with
VLAN interfaces rather than NIC's.

/Benny

Subject: Re: Re: several nics on the hn
Posted by Daniel Bauer on Fri, 07 Oct 2011 10:46:39 GMT
View Forum Message <> Reply to Message

Hi Benny,

From: "Benny Amorsen" <benny+usenet@amorsen.dk>
> "Daniel Bauer" <mlist@dsb-gmbh.de> writes:
>> I've several nics on the hostnode. Only the internal service nic have
>> an
>> internal IP. The other nics are without IPs and connected to
>> different
>> internal subnets and public www.
>>
>> I've read the differences between venet and veth
>> http://wiki.openvz.org/Differences_between_venet_and_veth
>> and want to use venet, but only venet0 is active in the hn, I think
>> this
>> is connected to eth0, but how to access the other nics?
>
> What we do is a bit simpler: Just add the appropriate NIC into the
> guest. This way the host loses access to the NIC and the guest can be
> configured in exactly the same way a non-virtualized server would be
> configured. Routing and firewalling is then done by our usual routers
> and firewalls, again exactly like it works for non-virtualized
> servers.
>
> To avoid having to put 50 NIC's in each VZ server we actually do it
> with

> VLAN interfaces rather than NIC's.

It's an really interesting solution. I've to look at the VLAN technic,
because I've never used it.

One thing was, that nobody - only the HN - could change the IP for a CT.
This issue couldn't be solved by VLAN or veth, so I thought to use
venet.

Now I think I'll prefer the bultin veth technic to solve my problem
right now.

Thanks a lot
Daniel

Subject: Re: several nics on the hn
Posted by Daniel Bauer on Fri, 07 Oct 2011 10:48:10 GMT
View Forum Message <> Reply to Message

Hi Esmé,

From: "Esmé de Wolf" <esme@elements.nl>
> When you want to use this kind of configuration:
>
> ---internal---> | hn | VEID 1
> ---NIC 2----> | | VEID 2
> ---NIC 3----> | | VEID 3
>
> And what you try is, f.e., to have the internal NIC only connecting to
> the
> hn, and NIC 2 to VEID 3 and NIC 3 to VEID 2, then you probably will
> need to
> route and firewall your config if you stick to venet.
>
> Using a bridged setup would mean the same security implications as
> using the
> setup above (firewalled). So that's not something to worry about.

I think I do it with veth, also if I prefered the venet interface,
because nobody could change the IP inside the CT.

Thanks
Daniel

> -----Oorspronkelijk bericht-----
> Van: users-bounces@openvz.org [mailto:users-bounces@openvz.org] Namens

> Daniel Bauer
> Verzonden: donderdag 6 oktober 2011 22:14
> Aan: users@openvz.org
> Onderwerp: Re: [Users] several nics on the hn
>
> Hi Esmé,
>
>> What's your setup? You have 1 'internal' NIC with an IP-address and
>> other NIC's without IP-address who you want to connect inside a
>> container, for what purpose?
>
> I've several nets:
> 1. internal service net, only available from/for the hostnode 2.
> internal
> LAN with intranet services for my users 3. DMZ 4. external IPs
>
> The host node should only be accessible in net 1, I don't want any
> routing
> or firewalling inside the hn, there should be no connection f.e.
> to net 4
>
>
>> If you use veth you could theoretically set up a bridge with one of
>> those
>> devices, that would be easiest in my opinion. But why would you
>> consist on
>> venet?
>
> In the mentioned article the are two advantages: security and
> performance
>
>
>> Probably with a little bit more information we can help you a bit
>> further.
>
>
> Thanks
> Daniel
>
>
>> -----Oorspronkelijk bericht-----
>> Van: users-bounces@openvz.org [mailto:users-bounces@openvz.org]
>> Namens
>> Daniel Bauer
>> Verzonden: donderdag 6 oktober 2011 15:02
>> Aan: users@openvz.org
>> Onderwerp: [Users] several nics on the hn
>>

>> Hello,
>>
>> I've several nics on the hostnode. Only the internal service nic have
>> an
>> internal IP. The other nics are without IPs and connected to
>> different
>> internal subnets and public www.
>>
>> I've read the differences between venet and veth
>> http://wiki.openvz.org/Differences_between_venet_and_veth
>> and want to use venet, but only venet0 is active in the hn, I think
>> this is
>> connected to eth0, but how to access the other nics?
>>
>> Thanks
>> Daniel
>>

Subject: Re: Re: several nics on the hn
Posted by Timh B on Fri, 07 Oct 2011 12:06:36 GMT
View Forum Message <> Reply to Message

Daniel,

On Fri, October 7, 2011 12:46, Daniel Bauer wrote:
> It's an really interesting solution. I've to look at the VLAN technic,
> because I've never used it.
>
> One thing was, that nobody - only the HN - could change the IP for a CT.
> This issue couldn't be solved by VLAN or veth, so I thought to use
> venet.
>
> Now I think I'll prefer the bultin veth technic to solve my problem
> right now.
>

I would also suggest you go this path, configure your "dedicated" hn-nic
(for this example, let's say it's eth0) as usual with the ip-address you
want.

Example (debian):
```
iface eth0 inet static
  address x.y.z.n
  netmask x.x.x.0
  gateway x.y.z.n

iface eth1 inet manual
```

```
iface eth1.100 inet manual
  vlan_raw_device eth0

iface eth1.200 inet manual
  vlan_raw_device eth0

iface vmbr100 inet manual
  bridge_ports eth1.100
  bridge_stp off
  bridge_fd 0

iface vmbr200 inet manual
  bridge_ports eth1.200
  bridge_stp off
  bridge_fd 0
```

--

Then, when creating your ct's you simple omit the --ipaddress flag on vzctl command and run vzctl <VEID> set --save --netif_add eth0,,,,vmbr100 and configure "eth0" within the CT.

This will put the ct-network in vlan100 on (hn) eth1 (which as you can see, has no ip-address configured) on the bridge vmbr100 as veth<VEID>.0 (confirm with "brctl show"). Note: you will have to configure your switch to send the vlan as "tagged" to the eth1 interface.

For your security concerns I suggest you look into mac-filtering or maybe check for mismatches between mac and ip addresses you have configured for the CT, the --netif_add command will generate a mac-address or you can set one manually.

The veth<VEID>.0 interface will also show up in the HN and you can do firewalling with something like this;

```
-A OUTPUT -o veth<VEID>.0 -s <IP> -j ACCEPT
-A OUTPUT -o veth<VEID>.0 -j DROP
```

(You will have to check the iptables-commands as I wrote them from the top of my head!)

Good luck!

-- Timh

Subject: Re: several nics on the hn
Posted by Antonio Querubin on Sat, 08 Oct 2011 06:54:05 GMT
View Forum Message <> Reply to Message

On Thu, 6 Oct 2011, Sam Trenholme wrote:

> However, what is missing is a RTFM on having a single container use
> different interfaces to route to different IP ranges. For example, a
> host that is a router with separate interfaces to 192.168.1.0/24 and
> 192.168.42.0/24, as well as a gateway to the internet, and we want a
> container on this host to access all three networks (for example, a
> container running Squid as a web proxy).

> So, here's my question: Is there a page out there which details
> exactly how to have an OpenVZ container use two or more different
> interfaces on the host machine?

http://wiki.openvz.org/VEs_and_HNs_in_same_subnets

The example covers 2 NICs. You can generalize it to N NICs.

Antonio Querubin
e-mail: tony@lavanauts.org
xmpp: antonioquerubin@gmail.com

Subject: Re: Re: several nics on the hn
Posted by Antonio Querubin on Sat, 08 Oct 2011 07:13:42 GMT
View Forum Message <> Reply to Message

On Fri, 7 Oct 2011, Daniel Bauer wrote:

> One thing was, that nobody - only the HN - could change the IP for a CT. This
> issue couldn't be solved by VLAN or veth, so I thought to use venet.

Hmmm. If you bridge the veth to the containers, the IP address for the
container is determined by the CT not the host.

Antonio Querubin
e-mail: tony@lavanauts.org
xmpp: antonioquerubin@gmail.com

Subject: Re: Re: several nics on the hn
Posted by Daniel Bauer on Sat, 08 Oct 2011 09:26:14 GMT
View Forum Message <> Reply to Message

From: "Antonio Querubin" <tony@lavanauts.org>

> On Fri, 7 Oct 2011, Daniel Bauer wrote:
>
>> One thing was, that nobody - only the HN - could change the IP for a
>> CT. This issue couldn't be solved by VLAN or veth, so I thought to
>> use venet.
>
> Hmmm. If you bridge the veth to the containers, the IP address for
> the container is determined by the CT not the host.

I know, this was the reason, that I'd like to take venet ...

Daniel

Subject: Re: Re: several nics on the hn
Posted by Daniel Bauer on Sat, 08 Oct 2011 09:39:25 GMT
View Forum Message <> Reply to Message

Hello Timh,

From: "Timh B" <timh@shiwebs.net>
> On Fri, October 7, 2011 12:46, Daniel Bauer wrote:
>> It's an really interesting solution. I've to look at the VLAN
>> technic,
>> because I've never used it.
>>
>> One thing was, that nobody - only the HN - could change the IP for a
>> CT.
>> This issue couldn't be solved by VLAN or veth, so I thought to use
>> venet.
>>
>> Now I think I'll prefer the bultin veth technic to solve my problem
>> right now.
>>
>
> I would also suggest you go this path, configure your "dedicated"
> hn-nic
> (for this example, let's say it's eth0) as usual with the ip-address
> you
> want.
>
> Example (debian):
> iface eth0 inet static
>   address x.y.z.n
>   netmask x.x.x.0
>   gateway x.y.z.n
>
> iface eth1 inet manual

>
> iface eth1.100 inet manual
> vlan_raw_device eth0
>
> iface eth1.200 inet manual
> vlan_raw_device eth0
>
> iface vmbr100 inet manual
> bridge_ports eth1.100
> bridge_stp off
> bridge_fd 0
>
> iface vmbr200 inet manual
> bridge_ports eth1.200
> bridge_stp off
> bridge_fd 0
>
> --
>
> Then, when creating your ct's you simple omit the --ipaddress flag on
> vzctl command and run vzctl <VEID> set --save --netif_add
> eth0,,,,vmbr100
> and configure "eth0" within the CT.
>
> This will put the ct-network in vlan100 on (hn) eth1 (which as you can
> see, has no ip-address configured) on the bridge vmbr100 as
> veth<VEID>.0
> (confirm with "brctl show"). Note: you will have to configure your
> switch
> to send the vlan as "tagged" to the eth1 interface.
>
> For your security concerns I suggest you look into mac-filtering or
> maybe
> check for mismatches between mac and ip addresses you have configured
> for
> the CT, the --netif_add command will generate a mac-address or you can
> set
> one manually.
>
> The veth<VEID>.0 interface will also show up in the HN and you can do
> firewalling with something like this;
>
> -A OUTPUT -o veth<VEID>.0 -s <IP> -j ACCEPT
> -A OUTPUT -o veth<VEID>.0 -j DROP
>
> (You will have to check the iptables-commands as I wrote them from the
> top
> of my head!)

Thanks a lot for this explanation.

Daniel

Subject: Re: several nics on the hn
Posted by Benny Amorsen on Mon, 10 Oct 2011 10:13:02 GMT
View Forum Message <> Reply to Message

"Daniel Bauer" writes:

> One thing was, that nobody - only the HN - could change the IP for a
> CT. This issue couldn't be solved by VLAN or veth, so I thought to use
> venet.

I see your point, however techniques for isolating physical servers are
quite mature (e.g. firewall rules or ACL's in routers). Using plain
VLAN's allows you to reuse those tools.

The discussion of all the other options is very interesting though.

/Benny

Subject: suPHP problem
Posted by Steffan on Wed, 12 Oct 2011 11:50:37 GMT
View Forum Message <> Reply to Message

When enabling suphp im getting the message that the site is using php 5.1.6
But im using solarspeed 5.2.13
Looking in the vsites php.ini file I see
extension_dir = "/home/solarspeed/php/lib/"
so look slike the righgt php.ini is there

so what is wrong ?

thanxs
