Subject: Advice needed on migration of Phys to VE
Posted by yettyn on Sun, 06 Jan 2008 14:14:29 GMT
View Forum Message <> Reply to Message

Hi,

I have a small private (physical) server online which I want to turn into a Virtualized one using openVZ. I have spent the last 2-3 days reading various resources about virtualisation in general and openVZ specifically, in preparation of the migrate and think I have understood most parts of it. But it's a lot of info to digest and I am not really sure how to put all pieces together for my specific situation, so I would be grateful for some advice/suggestions from someone with experience.

What I have is a box with a Intel Core 2 Duo E6750 (2.66Mhz) and 2GB RAM, and a 160GB SATA HDD. The box has 4 pub IP's on 1 interface (aliased eth0:0, eth0:1 etc.) hosting about 10 domains (using apache-2.2.6, proftpd, mySql5, PHP5 mainly), runs its own BIND dns and Shorewall Firewall 4.0.7 also installed.

My OS of choice is Gentoo and I have successfully been able to create an overlay ebuild of openVZ-2.6.22-ovz005.1 replacing my current Gentoo-Sources-2.6.22 kernel (Yes I know it's an unstable kernel but due to kernel changes between 2.6.18 and 2.6.22 I decided to go for the one comparative to what I had. So far I have seen no real problems, I have noticed in dmesg though the line 'VZDQ: sys/fs/quota creation failed' but it doesn't troubles me too much right now.). I have also successfully created a VE from a Gentoo template, but hasn't taken it further as I am unsure of next steps migrating IP's etc.

What I want to do is to split this box into 3 or possibly 4 VE's, both for better utilization of resources but also for securrity reasons. So I would like to run apache, php5 etc. in one VE, DNS and other "base" services in one, Postfix, amavisd etc. in one VE. Then is the question, with only 4 IP's available I guess I have to reserve 1 for HN leaving me with 3 for VE's?

If possible I would also like to run mysql in its own VE, but w/o access to more public IP's I guess I would need another nic (eth1) and go ahead with a layout including private IP's, NAT etc. I consider it wise though to wait with such a step and get the above layout working first.

I want to strip down services on HN to a bare minimum for administration of the VE's, but before that I need (at least most of) the data and services migrated. The box is co-located and although I have physically access to it office hours I usually manage it with ssh and webmin. If possible (which I think it is), I would also like to carry out the migration over ssh. Slight downtime of services etc. are not a problem.

I have read the wiki on migration from P2VE and although it have some usefull info I don't think it apply fully to me as I don't want to move the whole box into a VE but split it into 3-4 VE's and create them from fresh templates, install needed packages fresh etc.

Ok, maybe I have forgot something relevant but can't come to think about it now - insuch case just ask . My first step I think would be to move all web stuff into a first VE or?

tia,

Joakim

Subject: Re: Advice needed on migration of Phys to VE
Posted by kir on Sun, 06 Jan 2008 23:47:55 GMT
View Forum Message <> Reply to Message

I suggest you to have more than 3-4 VEs, following the "one VE per service" rule. It's not a problem that you only have 4 IP addresses -- the way to go is NAT and port forwarding, see http://wiki.openvz.org/Using_NAT_for_VE_with_private_IPs.

So, for example, in case of DNS, create a VE, assign some private IP (http://en.wikipedia.org/wiki/Private_network) to it, set up named in that VE, copy your named configuration from the host system to a new VE, test it. Then set up port forwarding so DNS queries will go to VE's named, not the host's one. If something goes wrong you can just remove the port forwarding rule until you fix the problem. When you're done, stop named on the host system.

The rule in question should look like this:
```
# iptables -t nat -A PREROUTING -p tcp -d ip_address --dport 53 \
  -i eth0 -j DNAT --to-destination ve_address:53
```

Here 53 is DNS port number, ip_address is IP your bind is currently listening at, and ve_address is your new VE IP. Do not forget to add the same rule but for udp (-p udp). If you are using bind9's rndc, do the same for port 953.

Subject: Re: Advice needed on migration of Phys to VE
Posted by yettyn on Mon, 07 Jan 2008 09:21:44 GMT
View Forum Message <> Reply to Message

Ok thanks for replying, I will try with private ip's, I just had the impression I needed another nic to mix private/public ip's on the same box but apparently not. Btw would be easier or more difficult to use a second nic (eth1) to set up this?

Another thing, I have Shorewall Firewall installed on HN to handle iptables rules, it might cause implications and would probably not be needed on HN at least after migration is done?

I have run into another problem as well but will open a separate treed on it.

/Joakim

P.S. a dot slipped in to the end of wiki url above so the link points to an empty wiki page. Maybe you should edit for others coming here.

Subject: Re: Advice needed on migration of Phys to VE
Posted by yettyn on Mon, 07 Jan 2008 16:11:45 GMT
View Forum Message <> Reply to Message

kir wrote on Mon, 07 January 2008 00:47
So, for example, in case of DNS, create a VE, assign some private IP (http://en.wikipedia.org/wiki/Private_network) to it, set up named in that VE, copy your named configuration from the host system to a new VE, test it. Then set up port forwarding so DNS queries will go to VE's named, not the host's one. If something goes wrong you can just remove the port forwarding rule until you fix the problem. When you're done, stop named on the host system.

I have a further question regarding this. I basically understand how it should be done but uncertain about few thing and as dns is a rather important part of the system I better ask before starting fiddle with it.

What I wonder about is how I handle the host name and ip for this VE in regards to the named.conf. In essence this VE host will replace HN host in a public sense, so how do I handle this in the zone file? Will I list this VE with a public IP A record or a CNAME alias?

As I understand it, setting things up this way I canget away with using only 1 public IP on this box, which will be for the HN, but this IP will basically also be the public interface for all VE hosts and I assume need to have this in the their zone files.

It's possible I complicate things unneccesarrily, but afaik my HN's FQDN is registered as a dns host so I think it must remain as a A record IP in dns, so how do I handle the dns VE - can I list it in zone file with same public IP as A record as well? I know it's possible to have 2 A records with same IP but different host name but I am no dns guru and is unsure about how it comes out in the end... kinda.

/Joakim

Subject: Re: Advice needed on migration of Phys to VE
Posted by yettyn on Mon, 07 Jan 2008 16:26:49 GMT
View Forum Message <> Reply to Message

and another thing, which nameserver do I give here
vzctl set 101 --nameserver 192.168.1.165 --save
for the dns VE, it's own internal IP or the HN public IP?

Just to make it clear, my box is collocated and a separate unit of 4 IP's within a subnet and manage my own dns for everything hosted on my box. I assume there is a dns above me belonging to my ISP that simply all my requests go though although I don't list this IP anywere in my config, just the gateway out of my little space.

Subject: Re: Advice needed on migration of Phys to VE
Posted by yettyn on Tue, 08 Jan 2008 14:21:04 GMT
View Forum Message <> Reply to Message

Ok I have managed to get VE_101 up and running on 192.168.0.101 and it can access internet as well as my current dns on HN. So first step completed

Still I am not sure what to do exactly with moving the dns to VE_101. I think I get it on the technical side, it's more the dns stuff that worries me... as the HN's hostname and ip is registered as my dns master so I kinda need to keep this somehow, either on HN or in VE, and as I am new to this vps thingy I also isn't sure if I miss something and simply makes it harder then it really is

If anyone here with deeper dns knowledge then me or already running a dns in a VE I am happy to get a helping hand.

/Joakim