On 04/17/2012 03:07 PM, Brad Alexander wrote:
> Thanks Kir.
>
> On Tue, Apr 17, 2012 at 3:29 AM, Kir Kolyshkin<kir@openvz.org> wrote:
>> On 04/14/2012 12:07 AM, Brad Alexander wrote:
>>> I just found out through the proxmox-ve forums that running ntp on a
>>> container is considered a Bad Thing.
>>
>> Not necessarily. In fact, it's a good thing to run ntpd inside a container,
>> it's just you need to
>>
>> 1. Have only ONE container doing that.
> So that one container can be Container 0 (the HN)?

Yes, but from the privilege separation perspective it might make sense
to have a dedicated container for that, so you don't clog HN with all
sorts of services and daemons.

>
>> 2. Grant that container sys_time capability, so it will be able to set
>> system time.
> Perhaps I misunderstood the sys_time flag, it was my understanding
> that it was better to turn off ntp on the containers

Right, it doesn't make sense to run ntpd in more than one container (or HN).

> , make sure it is
> on in container 0 (the hardware node)

Right. Or any other _single_ container.

> , then turn on sys_time on the
> remaining containers.

Ughm. That way, root user of any of those container can change system
time (and affect other users of CTs on the same HN).

>
>> This is because time is not virtualized, ie all the containers share the
>> same time (because indeed there's only one time -- time zones of course can
>> be different).
> Thanks,
> --b