Subject: a newbie question
Posted by cheetah on Sun, 17 Jun 2012 10:25:39 GMT
View Forum Message <> Reply to Message

Hi guys,

I am a newbie to openvz and preparing to deploy it in my production environment to give each user a container. I have the following concerns now.

1. Can user load kernel modules in the guest container without influencing the host kernel or other container's kernel? As far as I understand, all the containers share the same kernel of the host. So I am wondering if this is possible?

2. Or how is the container's security isolation? Can I give user root access in the container? Is there any hack that he/she can use root in the container to attack the host or other containers?

3. Does openvz kernel support kvm?

4. What is recommended distro of Linux to install openvz? I am now using CentOS 6.2. How about Debian?

Thanks a lot for answering my stupid questions.

Regards,
Peter

Subject: Re: a newbie question
Posted by Martin Dobrev on Sun, 17 Jun 2012 10:56:12 GMT
View Forum Message <> Reply to Message

Martin Dobrev

Sent from iPhonespam SPAMSPAM 4

On 17.06.2012, at 13:25, cheetah <xuwh06@gmail.com> wrote:

> Hi guys,
>

Hi Peter,

> I am a newbie to openvz and preparing to deploy it in my production environment to give each user a container. I have the following concerns now.
>

> 1. Can user load kernel modules in the guest container without influencing the host kernel or other container's kernel? As far as I understand, all the containers share the same kernel of the host. So I am wondering if this is possible?
>

Some modules can be shared from the host sytem to the containers. More info in the vzctl man page.

> 2. Or how is the container's security isolation? Can I give user root access in the container? Is there any hack that he/she can use root in the container to attack the host or other containers?
>
It's impossible to gain host system access using a kernel bug as far as I know. Some kernel exploits are still able to crash the hole system. Giving root in the container will be considered as secure as giving root on physical server.
> 3. Does openvz kernel support kvm?
>
It's possible to have Xen and KVM compiled in the OVZ kernel but you'll need to compile it yourself.
> 4. What is recommended distro of Linux to install openvz? I am now using CentOS 6.2. How about Debian?
>
Mainstream kernel development follows the RHEL kernel branches, so best for you will be CentOS. I have some production systems on it too.
> Thanks a lot for answering my stupid questions.
>
I hope my info helps.
> Regards,
> Peter
P.S. There is no need to write to the devel list directly for user questions.

Subject: Re: a newbie question
Posted by cheetah on Sun, 17 Jun 2012 11:10:42 GMT
View Forum Message <> Reply to Message

Thanks a lot for the info, Martin.

Nice to know Openvz kernel is based on RHEL6. I am wondering how fast it is
released after a new release of RHEL?

Thanks.
Peter

On Sun, Jun 17, 2012 at 6:56 PM, Martin Dobrev <martin@dobrev.eu> wrote:

>
>
> Martin Dobrev

>
> Sent from iPhonespam SPAMSPAM 4
>
> On 17.06.2012, at 13:25, cheetah <xuwh06@gmail.com> wrote:
>
> > Hi guys,
> >
>
> Hi Peter,
>
> > I am a newbie to openvz and preparing to deploy it in my production
> environment to give each user a container. I have the following concerns
> now.
> >
> > 1. Can user load kernel modules in the guest container without
> influencing the host kernel or other container's kernel? As far as I
> understand, all the containers share the same kernel of the host. So I am
> wondering if this is possible?
> >
>
> Some modules can be shared from the host sytem to the containers. More
> info in the vzctl man page.
>
> > 2. Or how is the container's security isolation? Can I give user root
> access in the container? Is there any hack that he/she can use root in the
> container to attack the host or other containers?
> >
> It's impossible to gain host system access using a kernel bug as far as I
> know. Some kernel exploits are still able to crash the hole system. Giving
> root in the container will be considered as secure as giving root on
> physical server.
> > 3. Does openvz kernel support kvm?
> >
> It's possible to have Xen and KVM compiled in the OVZ kernel but you'll
> need to compile it yourself.
> > 4. What is recommended distro of Linux to install openvz? I am now using
> CentOS 6.2. How about Debian?
> >
> Mainstream kernel development follows the RHEL kernel branches, so best
> for you will be CentOS. I have some production systems on it too.
> > Thanks a lot for answering my stupid questions.
> >
> I hope my info helps.
> > Regards,
> > Peter
> P.S. There is no need to write to the devel list directly for user
> questions.

Subject: Re: a newbie question
Posted by Christian Blaich on Sun, 17 Jun 2012 11:20:58 GMT
View Forum Message <> Reply to Message

Check proxmox, ovz kvm modules already loaded in the Kernel. Easy to handle via console and also via Web. Based on debian. Good howtos!

Mobil verfasst

Am 17.06.2012 um 13:10 schrieb cheetah <xuwh06@gmail.com>:

> Thanks a lot for the info, Martin.
>
> Nice to know Openvz kernel is based on RHEL6. I am wondering how fast it is released after a new release of RHEL?
>
> Thanks.
> Peter
>
> On Sun, Jun 17, 2012 at 6:56 PM, Martin Dobrev <martin@dobrev.eu> wrote:
>
>
> Martin Dobrev
>
> Sent from iPhonespam SPAMSPAM 4
>
> On 17.06.2012, at 13:25, cheetah <xuwh06@gmail.com> wrote:
>
> > Hi guys,
> >
>
> Hi Peter,
>
> > I am a newbie to openvz and preparing to deploy it in my production environment to give each user a container. I have the following concerns now.
> >
> > 1. Can user load kernel modules in the guest container without influencing the host kernel or other container's kernel? As far as I understand, all the containers share the same kernel of the host. So I am wondering if this is possible?
> >
>
> Some modules can be shared from the host sytem to the containers. More info in the vzctl man page.
>
> > 2. Or how is the container's security isolation? Can I give user root access in the container? Is there any hack that he/she can use root in the container to attack the host or other containers?
> >

> It's impossible to gain host system access using a kernel bug as far as I know. Some kernel exploits are still able to crash the hole system. Giving root in the container will be considered as secure as giving root on physical server.
> > 3. Does openvz kernel support kvm?
> >
> It's possible to have Xen and KVM compiled in the OVZ kernel but you'll need to compile it yourself.
> > 4. What is recommended distro of Linux to install openvz? I am now using CentOS 6.2. How about Debian?
> >
> Mainstream kernel development follows the RHEL kernel branches, so best for you will be CentOS. I have some production systems on it too.
> > Thanks a lot for answering my stupid questions.
> >
> I hope my info helps.
> > Regards,
> > Peter
> P.S. There is no need to write to the devel list directly for user questions.

Subject: Re: a newbie question
Posted by LightDot on Sun, 17 Jun 2012 13:03:58 GMT
View Forum Message <> Reply to Message

Hello Martin and Peter,

On Sun, Jun 17, 2012 at 12:56 PM, Martin Dobrev <martin@dobrev.eu> wrote:
>
>
> Martin Dobrev
>
> Sent from iPhonespam SPAMSPAM 4
>
> On 17.06.2012, at 13:25, cheetah <xuwh06@gmail.com> wrote:
>
>> Hi guys,
>>
>
> Hi Peter,
>
>> I am a newbie to openvz and preparing to deploy it in my production environment to give each user a container. I have the following concerns now.
>>
>> 1. Can user load kernel modules in the guest container without influencing the host kernel or other container's kernel? As far as I understand, all the containers share the same kernel of the host. So I am wondering if this is possible?
>>
>

> Some modules can be shared from the host sytem to the containers. More info in the vzctl man page.
>

Users can't load modules from within the guest containers. Modules can be loaded on the hardware node and they will be available to all containers. Usability depends on the specific module, guest containers might not be able to use some of them.

>> 2. Or how is the container's security isolation? Can I give user root access in the container? Is there any hack that he/she can use root in the container to attack the host or other containers?
>>
> It's impossible to gain host system access using a kernel bug as far as I know. Some kernel exploits are still able to crash the hole system. Giving root in the container will be considered as secure as giving root on physical server.

I would say giving your customers root access to a container is pretty safe. In case of kernel exploits or bugs, there might be a certain risk. For example, recent watchdog kernel bug enabled container users to reboot the node. In my experience, such bugs are quickly dealt with and few and far between. I haven't been bitten by any yet.

>> 3. Does openvz kernel support kvm?
>>
> It's possible to have Xen and KVM compiled in the OVZ kernel but you'll need to compile it yourself.

I don't think this is true, perhaps I'm misunderstanding what you're saying. KVM is a part of the mainline kernel and a part of Red Hat kernels, I don't think openvz is in any way stripping it out. KVM should work sam as it works on a regular Red hat kernel, shouldn't it?

>> 4. What is recommended distro of Linux to install openvz? I am now using CentOS 6.2. How about Debian?
>>
> Mainstream kernel development follows the RHEL kernel branches, so best for you will be CentOS. I have some production systems on it too.

I'd recommend CentOS or Scientific Linux 6.x. If you'd like to use Debian, I'd recommend using Red Hat version of openvz kernel with it too.

>> Thanks a lot for answering my stupid questions.
>>
> I hope my info helps.
>> Regards,
>> Peter
> P.S. There is no need to write to the devel list directly for user questions.
Regards to all...

Subject: Re: a newbie question
Posted by Aleksandar Ivanisevic on Mon, 18 Jun 2012 09:41:52 GMT
View Forum Message <> Reply to Message

Christian Blaich <christian@blaich.eu>
writes:

> Check proxmox, ovz kvm modules already loaded in the Kernel. Easy to
> handle via console and also via Web. Based on debian. Good howtos!

To be fair, kvm modules are also included in the stock ovz rhel6 kernel.

[...]
