Subject: How do I mount /tmp on VEs with noexec,nosuid options?
Posted by aseques on Fri, 09 Nov 2007 16:56:19 GMT
View Forum Message <> Reply to Message

Following http://kb.swsoft.com/article_130_648_en.html
I get " unrecognized option `--bindmount_add'" so I guess that in
openVZ it works different.
There was no message in the list related to this.
Anyone knows if there is a command for that?

Subject: Re: How do I mount /tmp on VEs with noexec,nosuid options?
Posted by kir on Mon, 12 Nov 2007 12:46:53 GMT
View Forum Message <> Reply to Message

Joan wrote:
> Following http://kb.swsoft.com/article_130_648_en.html
> I get " unrecognized option `--bindmount_add'" so I guess that in
> openVZ it works different.
> There was no message in the list related to this.
> Anyone knows if there is a command for that?
>

Try to search forum.openvz.org. If you will find the working solution,
please document it on wiki.openvz.org.

Thanks!

Subject: Re: How do I mount /tmp on VEs with noexec,nosuid options?
Posted by aseques on Mon, 12 Nov 2007 21:46:50 GMT
View Forum Message <> Reply to Message

2007/11/12, Kir Kolyshkin <kir@openvz.org>:
> Joan wrote:
> > Following http://kb.swsoft.com/article_130_648_en.html
> > I get " unrecognized option `--bindmount_add'" so I guess that in
> > openVZ it works different.
> > There was no message in the list related to this.
> > Anyone knows if there is a command for that?
> >
>
> Try to search forum.openvz.org. If you will find the working solution,
> please document it on wiki.openvz.org.

I downloaded the mailing list archives since 2005 and couldn't find a
solution, now I'm looking in the forums and there's something at least

interesting:
http://forum.openvz.org/index.php?t=msg&goto=12999&&srch=noexec#msg_12999

Quote:

white:/# mount -t tmpfs -o noexec,nosuid tmpfs /tmp/
white:/# cat /proc/mounts
simfs / simfs rw 0 0
proc /proc proc rw 0 0
sysfs /sys sysfs rw 0 0
devpts /dev/pts devpts rw 0 0
tmpfs /dev/shm tmpfs rw 0 0
tmpfs /tmp tmpfs rw,nosuid,noexec 0 0

It seems to do the trick

Next step would be to permanently add it to the fstab
# UNCONFIGURED FSTAB FOR BASE SYSTEM
tmpfs /tmp tmpfs noexec,nosuid 0 0
tmpfs /var/tmp tmpfs noexec,nosuid 0 0

At this moment I can't reboot the veid, tomorrow I'll try and see if data in
fstab remains in the text file after rebooting.

---

Subject: Re: How do I mount /tmp on VEs with noexec,nosuid options?
Posted by aseques on Tue, 13 Nov 2007 11:20:38 GMT
View Forum Message <> Reply to Message

2007/11/12, Joan <aseques@gmail.com>:
>
>
>
> 2007/11/12, Kir Kolyshkin <kir@openvz.org>:
> > Joan wrote:
> > > Following http://kb.swsoft.com/article_130_648_en.html
> > > I get " unrecognized option `--bindmount_add'" so I guess that in
> > > openVZ it works different.
> > > There was no message in the list related to this.
> > > Anyone knows if there is a command for that?
> > >
> >
> > Try to search forum.openvz.org. If you will find the working solution,
> > please document it on wiki.openvz.org .
>
> I downloaded the mailing list archives since 2005 and couldn't find a
> solution, now I'm looking in the forums and there's something at least
> interesting:

> http://forum.openvz.org/index.php?t=msg&goto=12999&&srch=noexec#msg_12999
>
> Quote:
>
> white:/# mount -t tmpfs -o noexec,nosuid tmpfs /tmp/
> white:/# cat /proc/mounts
> simfs / simfs rw 0 0
> proc /proc proc rw 0 0
> sysfs /sys sysfs rw 0 0
> devpts /dev/pts devpts rw 0 0
> tmpfs /dev/shm tmpfs rw 0 0
> tmpfs /tmp tmpfs rw,nosuid,noexec 0 0
>
> It seems to do the trick
>
> Next step would be to permanently add it to the fstab
> # UNCONFIGURED FSTAB FOR BASE SYSTEM
> tmpfs /tmp tmpfs noexec,nosuid 0 0
> tmpfs /var/tmp tmpfs noexec,nosuid 0 0
>
> At this moment I can't reboot the veid, tomorrow I'll try and see if data
> in fstab remains in the text file after rebooting.
>

Ok, I can confirm it works as expected.
I rebooted the VeID a couple of times and the changes in fstab are kept.

Even though, wouldn't be nice if there was a parameter to vzctl --bindmount_add
that could do like in virtuozzo.
I wouldn't be so difficult to create an script to replace the appropiate
fields in the /vz/private/veid/root/fstab and add it as a function in the
vzctl.
I'll gladly do the script if it was interestin.

---

Subject: Re: How do I mount /tmp on VEs with noexec,nosuid options?
Posted by rmello on Wed, 14 Nov 2007 06:27:19 GMT
View Forum Message <> Reply to Message

On Nov 9, 2007 9:56 AM, Joan <aseques@gmail.com> wrote:
> Following http://kb.swsoft.com/article_130_648_en.html
> I get " unrecognized option `--bindmount_add"' so I guess that in
> openVZ it works different.
> There was no message in the list related to this.
> Anyone knows if there is a command for that?

Have you tried the following:

HN# vzctl start 101
HN# mount -n --bind -o nosuid,noexec /tmp /path/to/vz/root/101/tmp

Notice the -n flag. That is necessary, and it'll cause mount not to update /etc/mtab, so the bind mount won't show up in the output of `mount`, but it will in the output of /proc/mounts.

Once you've got the mount and unmount working, you can put the commands into /etc/vz/conf/101.mount and 101.umount (need to be executable and have appropriate shebangs). The .umount file particularly seems to executed when you start the VE too, so in it you need to check if the FS is mounted before trying to unmount. I have something like this in my 101.umount:

```
---------
#!/bin/bash
VEID=101
MNTPATH="/path/to/vz/root/${VEID}/tmp"
mnt=`grep ${MNTPATH} /proc/mounts | wc -l`

if [ ${mnt} -eq 1 ]; then
    umount ${MNTPATH}
fi
-------
```

And 101.mount can be a very simple:

```
-------
#!/bin/bash
VEID=101
MNTPATH="/path/to/vz/root/${VEID}/tmp"
mount -n --bind /tmp ${MNTPATH}
-------
```

Let us know if that works for you. I use the above technique, which I learned long ago, to bind different filesystems to my VEs, including remote filesystems. Be careful with permissions. I sometimes create a per-ve directory in the source, then bind mount that one to the named VE, to keep things tidy.

Roberto
http://blog.divisiblebyfour.org/