## Subject: OpenVZ 7 + how to make /tmp noexec,nosuid,nodev with quota limit?
Posted by ccto on Thu, 11 Apr 2019 15:49:57 GMT

I am finding a solution to create a "secure tmp" for container on OpenVZ 7 platform.

Target: create a (e.g.) 2GB partition for /tmp with noexec,nosuid,nodev enabled.

In OpenVZ 6 ones, I used script to bind-mount /tmp to separate simfs directory with vzquota limit.

However, in OpenVZ 7,
- prlctl device-add does not have mount options.
- Browsing the source, manually adjusting /vz/private/{UUID}/ve.conf mnt_opts in DISK directive , and restart VE.  It seems not work too.
- No simfs/vzquota support in OpenVZ 7.

So frustrating.

Any solutions?  Please advise.


Thank you
Regards
George


## Subject: Re: OpenVZ 7 + how to make /tmp noexec,nosuid,nodev with quota limit?
Posted by ccto on Tue, 23 Apr 2019 07:46:55 GMT

Finally, I managed to
- create a file as a block device (dd), and mkfs.ext4 it
- mount it as loop,rw,nodev,nosuid,noexec
- bind-mount it inside guest /tmp to that folder.

It looks work.