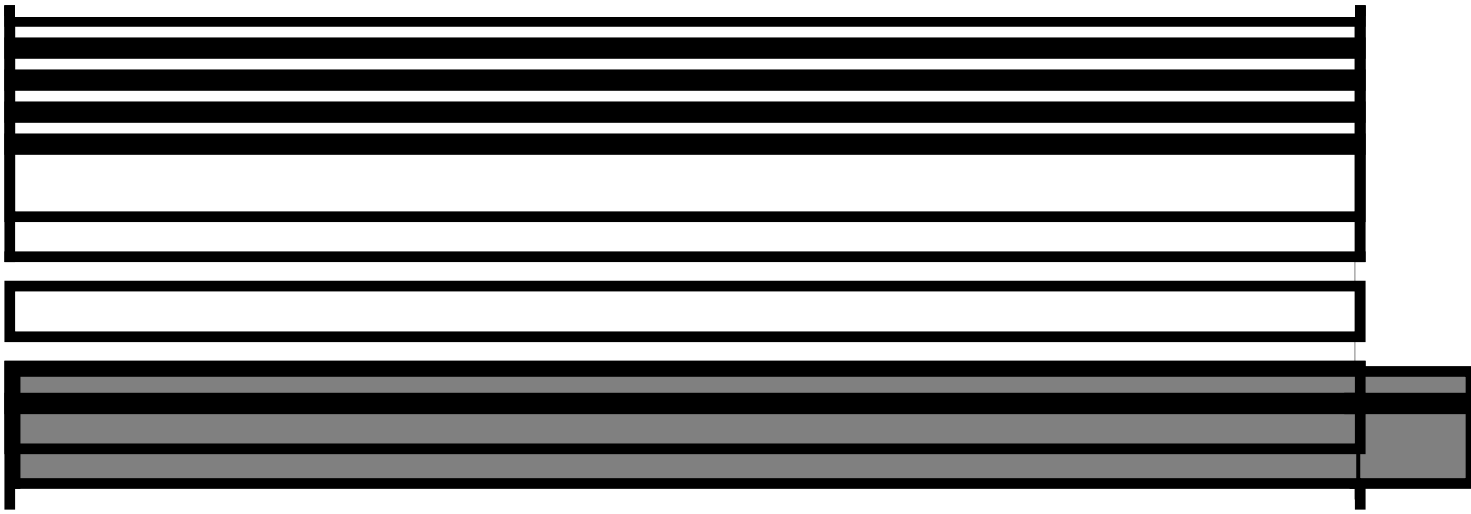
Securing /tmp and shm partitions

Article Number: 681 | Rating: Unrated | Last Updated: Fri, May 15, 2020 12:03 PM

Securing /tmp and /dev/shm is a nice practice. Lots of programs and scripts have access in there. So you don’t want code, malicious or not to run in there, trying to get root permissions or snoop on you.

Temporary storage directories such as /tmp, /var/tmp and /dev/shm provide storage space for malicious executables.
Crackers and hackers store executables in /tmp. Malicious users can use temporary storage directories to execute unwanted program and crack your server.

First because I forget, let’s bind /var/tmp to /tmp in **/etc/fstab**

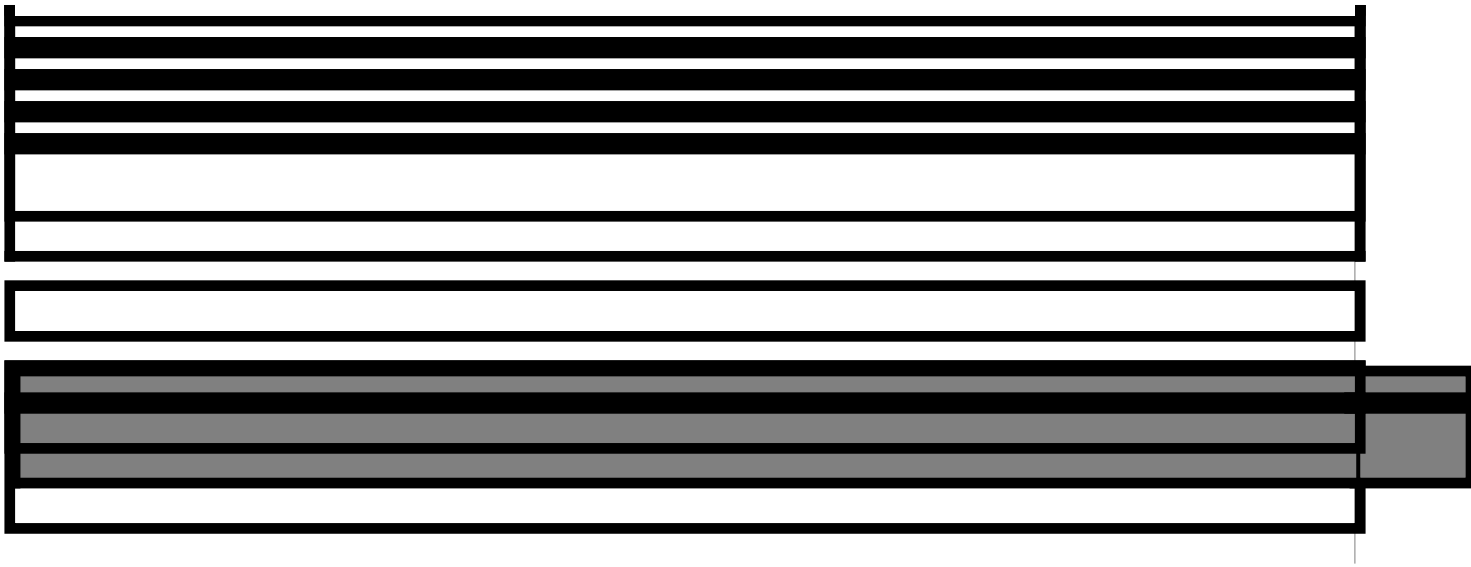


Now we deal with /tmp only.

Update 28/03/2015: That practice was for many unstable and criticized also by many. Unfortunately for them, I was vindicated when even OpenBSD in the upcoming version does the same for the very same reasons. Security.

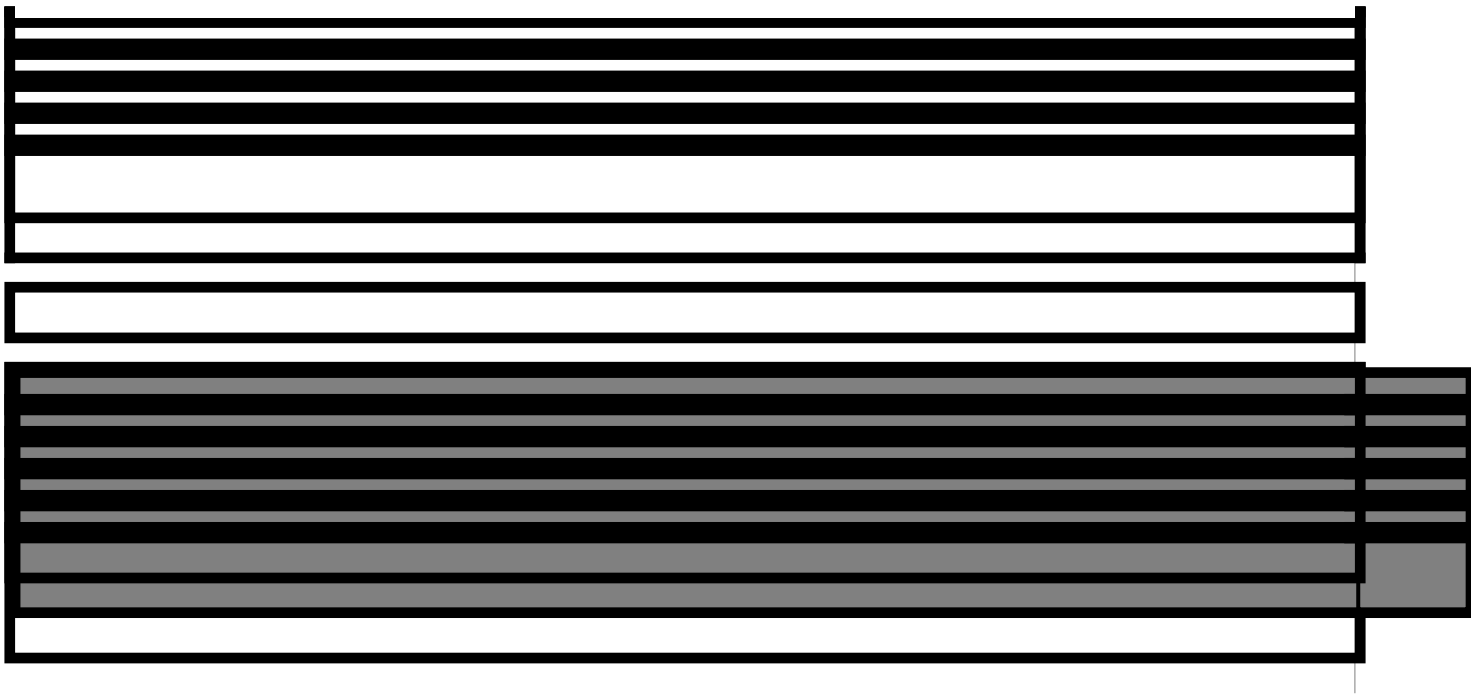
> *Security improvements:*
>
> - */var/tmp is now a symbolic link to /tmp, as a first step towards reducing the "fill it up" attack surface against the /var partition.*

If it's a separate partition we only need a

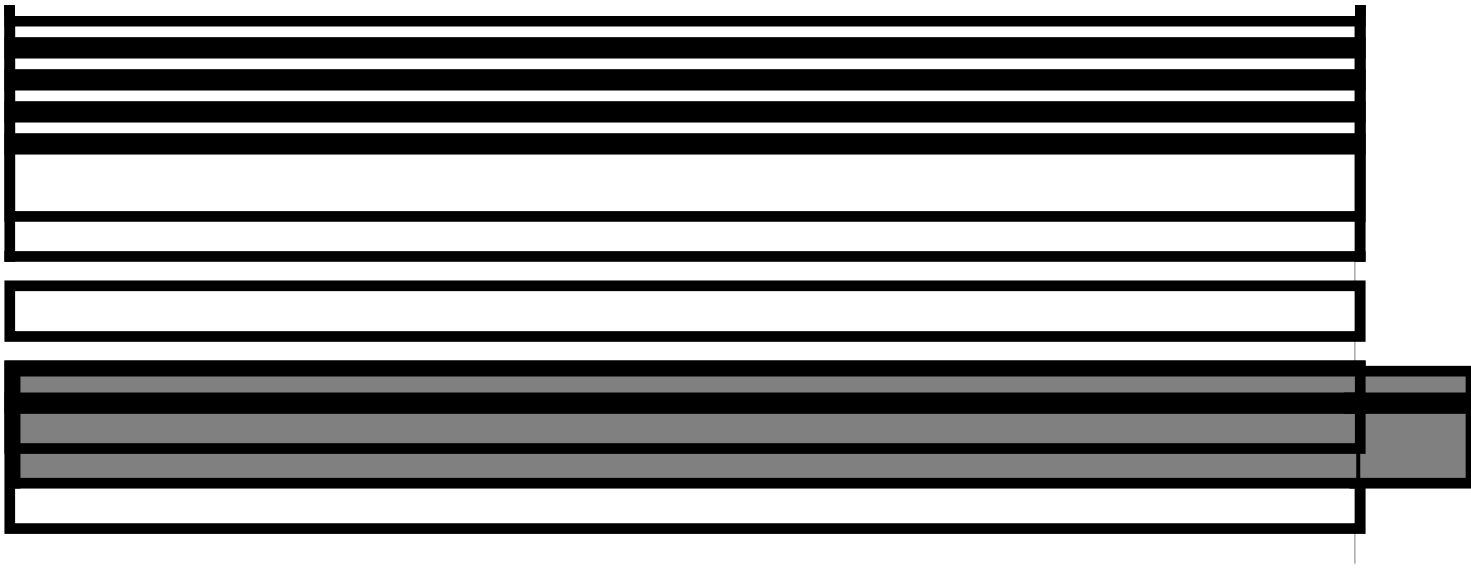


If it's not, we will create an image for it. The example is for 4GB, tune it as you

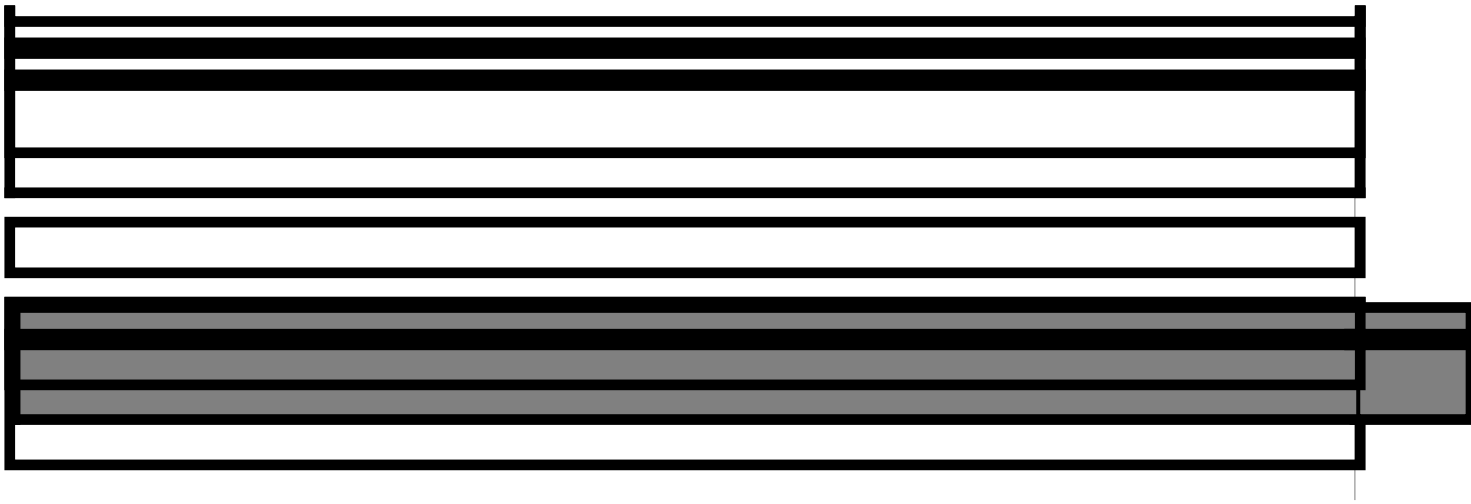
like.



Modify /tmp line as follows:



You should to the same for shm:



Edit your /etc/fstab:
nano /etc/fstab

change:
“none /dev/shm tmpfs defaults,rw 0 0” to
“none /dev/shm tmpfs defaults,nosuid,noexec,rw 0 0”

Remount /dev/shm:
mount -o remount /dev/shm
It should be fine now.