Subject: Need to extract data from backup
Posted by madsmao on Sun, 31 May 2015 12:47:28 GMT
View Forum Message <> Reply to Message

Unfortunately, one of our containers got hacked, and the intruders have managed to corrupt an important MySQL database. Now, I do have a backup of the container that got hacked, but when I try to restore the backup using vzrestore, the process simply exists after a while without any exit code. I suspect that this is because it's a really big backup (300G+), but could also be because the backup is incomplete.

Now, what I would like to do is to somehow mount the filesystem inside the tar file (on the host), and see if I can find the MySQL database that I am looking for. Is this in any way possible? I have obviously searched around quite a bit, but I have not been able to find any useful information.

I do know that the container is using simfs, and that I was able to mount the backup (TAR-file) using archivemount. However, the only thing that gives me access to is 2 large files inside the backup labelled root.hdd.{SOME-LONG-HASH}. I assume that these files are both simfs images, but how would I go about mounting them?