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?

Subject: Re: Need to extract data from backup
Posted by Paparaciz on Sun, 31 May 2015 18:20:53 GMT
View Forum Message <> Reply to Message

it is ploop image file. dunno how backup is consistent but maybe you are lucky.
documentation regarding this:
https://wiki.openvz.org/Ploop

in general:
Quote:
ploop mount /ploop.image
Since this point, /dev/ploopXXXX is operable. One can read/write any data from/to it (e.g. with "dd"), manipulate partition table on it (with parted, since ploop uses GUID Partition Table, or GPT), format it with mkfs.ext4 and mount it on some mount-point. In the other words, since now /dev/ploop0 can be used as any other ordinary block device.

if you will have some problems I recommend you contact paid support if it covers questions like this:
http://www.odin.com/support/virtualization-suite/openvz/

or any other company which knows ploop quite well.

Subject: Re: Need to extract data from backup
Posted by madsmao on Sun, 31 May 2015 18:29:18 GMT
View Forum Message <> Reply to Message

Thank you for your reply.

I tried issuing the following command from within my mounted tar file:

[root@server18 root.hdd]# ploop mount root.hdd.\{4410aa10-0157-437d-b0c5-0efc3f0c0b91\}
Adding delta dev=/dev/ploop55202 img=root.hdd.{4410aa10-0157-437d-b0c5-0efc3f0c0b91} (rw)
Error in add_delta (ploop.c:1174): Can't open file
root.hdd.{4410aa10-0157-437d-b0c5-0efc3f0c0b91}: Invalid argument

As you can see, the mount didn't succeed. Am I missing something, or could this be a sign that the image is corrupted?

I guess it could also be because I haven't extrated the TAR-file first. Would it be an idea to try that?

Subject: Re: Need to extract data from backup
Posted by Paparaciz on Sun, 31 May 2015 18:53:26 GMT
View Forum Message <> Reply to Message

tar file is archive so yes, you have to extract it first.

Subject: Re: Need to extract data from backup
Posted by madsmao on Mon, 01 Jun 2015 04:37:20 GMT
View Forum Message <> Reply to Message

So, I managed to mount /dev/plopXXXXX after extracting the TAR-file. That's obviously great. However, my fairly limited knowledge about dealing with block devices means I am not entirely sure what to do from here. Essentially, I would like to do something like this:

- List the file contents on the device
- Search through the contents to find what I am looking for
- Extract only the information I need

How would I go about doing that? Any input is greatly appreciated.
