KeyHelp®
Server Control Panel

HowTo – KeyHelp- Restic- Backup Restore

Instructions for the complete restore of a Restic server backup

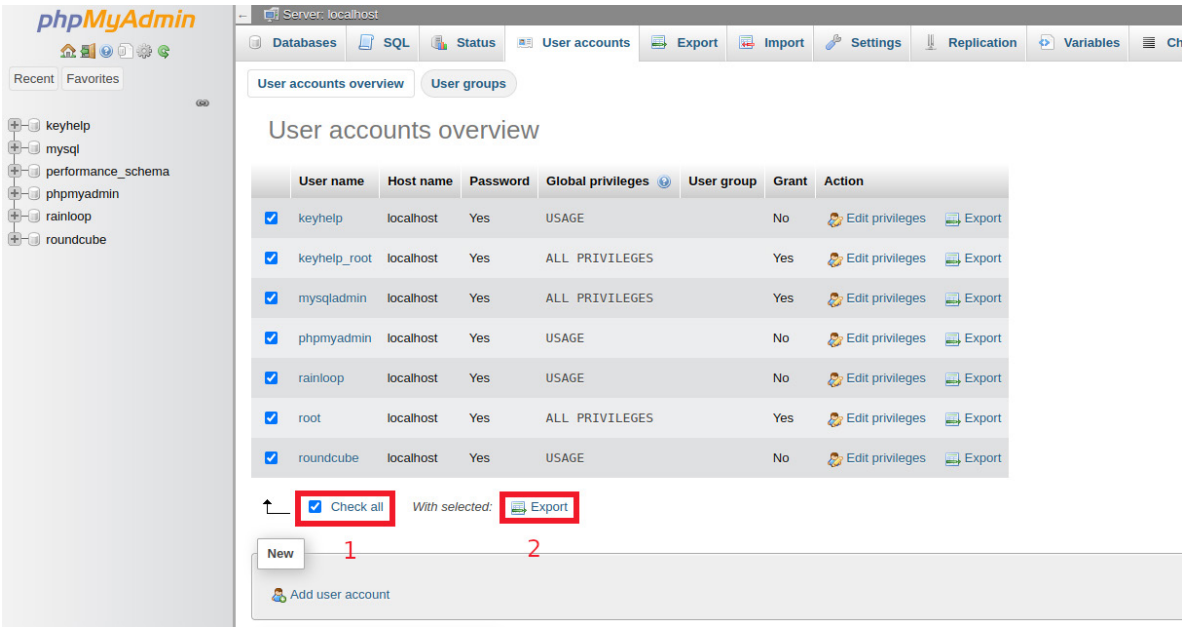
Preparation

1) Basic installation of new system with KeyHelp

2) Backup repository created and scanned in the new KeyHelp backup management

3) Backup of the current mySQL user configuration

- → e.g. export via PHPmyAdmin -> user accounts
- → it is best to copy the displayed commands and save them in a text file
- → is used to restore the passwords of KeyHelp, Roundcube etc. that were newly set during reinstallation



4) Stop mail services

- → service postfix stop
- → service dovecot stop

Restore

1a) Restore of users and groups

To do this, restore the `/etc` folder from the desired backup.

Important!

Do not restore the folder to the original path, but use the option "alternative path".

Author Florian Cheno / as of: 1st of March 2024

HowTo – KeyHelp- Restic- Backup Restore

Here you enter any path, e.g. `/restore` .

Now edit the files passwd and shadow in this restored folder and remove all system users.
Only the KeyHelp users must then remain.

Examples:

```
# cat /restore/etc/passwd
user1:x:5002:5002::/home/users/user1/:/bin/false
user2:x:5003:5003::/home/users/user2/:/bin/false
user3:x:5004:5004::/home/users/user3/:/bin/false
```

```
# cat /restore/etc/shadow
user1:$6$rounds=100000$z0xC2rvcOhKWle5Q$MicTuwQajK9jPAWfwcw8GUWa2JadODO5X3AD3FTwVXXro1nRtsvzcCE-
D2YEvBmdcSARL5UD8tnHngqW37/wFO/:19297:0:99999:7:::
```

```
user2:$6$rounds=100000$YzPJKEU4xmbGw6nH$jk2CpR3GXB3ZIl/8jhbHBEe8kZIqCUdnnbm4AnU51RDyz2VsHZAfRxd-
6VX9h4f7zDYJymQf/bKpt7./Y520ld0:19297:0:99999:7:::
```

```
user3:$6$rounds=100000$fFLuNe0IV.mibd4r$UKJDqJX5Zn0Zu5IpH0B1.aQVtJ0zuinAwGUh0DN.t0N3BXNws4TfAO-
DUbVbBvDtR2bp3haYdlpa9D8L7X9Iu70:19297:0:99999:7:::
```

These files are now attached to their respective equivalents:

```
cat /restore/etc/passwd >> /etc/passwd
```

```
cat /restore/etc/shadow >> /etc/shadow
```

Proceed in the same way with the group and gshadow files, with the difference that the KeyHelp groups are also copied:

```
# cat /restore/etc/group
keyhelp_file_manager:x:1001:user1,user2,user3
keyhelp_nossh:x:1002:user1,user2,user3
keyhelp_noftp:x:1003:
keyhelp_suspended:x:1004:
keyhelp_chroot:x:1005:
user1:x:5002:
user2:x:5003:
user3:x:5004:
```

```
# cat /restore/etc/gshadow
keyhelp_file_manager:!::user1,user2,user3
keyhelp_nossh:!::user1,user2,user3
keyhelp_noftp:!::
```

Author Florian Cheno / as of: 1st of March 2024

HowTo – KeyHelp- Restic- Backup Restore

```
keyhelp_suspended:!::
keyhelp_chroot:!::
user1:!::
user2:!::
user3:!::
```

Before appending to the actual system files `/etc/group` and `/etc/gshadow` it is important to remove the KeyHelp groups from these files, as they would otherwise be duplicated.

```
# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
. . .
keyhelp_file_manager:x:1001:
keyhelp_nossh:x:1002:
keyhelp_noftp:x:1003:
keyhelp_suspended:x:1004:
keyhelp_chroot:x:1005:
. . .
clamav:x:121:amavis
amavis:x:122:clamav
debian-spamd:x:123:
```

```
# cat /etc/gshadow
root:x:0:
daemon:x:1:
bin:x:2:
. . .
keyhelp_file_manager:!::
keyhelp_nossh:!::
keyhelp_noftp:!::
keyhelp_suspended:!::
keyhelp_chroot:!::
. . .
postfix:!::
postdrop:!::
```

Now append the edited files:

```
cat /restore/etc/group >> /etc/group
```

```
cat /restore/etc/gshadow >> /etc/gshadow
```

Author Florian Cheno / as of: 1st of March 2024

HowTo – KeyHelp- Restic- Backup Restore

1b) Restore KeyHelp's internal encryption

This is used, for example, when using 2-factor authentication. But also in other places, so it is definitely recommended to carry out this step.

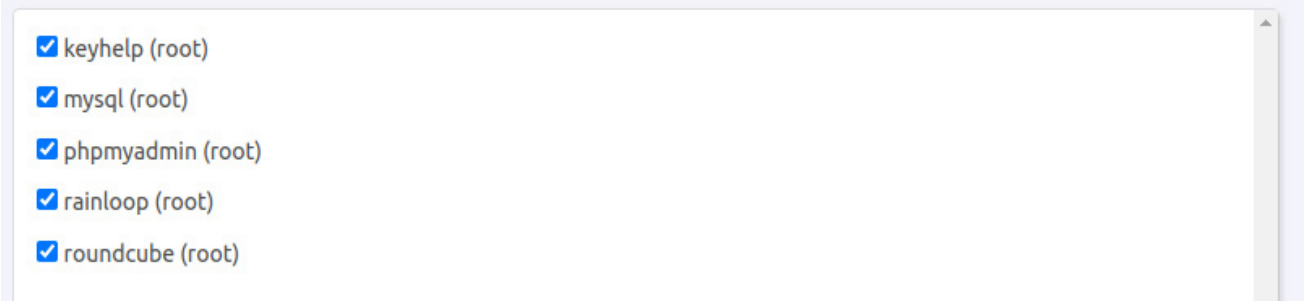
To do this, copy the "encryption" section from the file `/restore/etc/keyhelp/config/config.json` and replace the entry in the file `/etc/keyhelp/config/config.json` with it:

```
"encryption": {
        "base": "12345samecombinationonmyluggage"
    }
```

After the change, the backup repository in KeyHelp must be deleted and created again!

2) Restore of the default databases

Click on "restore backup" in the new backup management and restore the default databases keyhelp, mysql, phpmyadmin, rainloop and roundcube.



After completing the recovery, restart the database server once. Now a call to KeyHelp should be acknowledged with a database error.
This is the time to re-enter the commands saved in point 3 of the preparation via the MySQL command line to set the MySQL user passwords again.
Complete the entries with "`flush privileges;`" or restart the database server.

KeyHelp should now be accessible again and all elements such as users and domains should be visible in KeyHelp.

3) Restore of user data

It may be necessary to create the backup repository again, as a different KeyHelp config is now active.

Furthermore, all necessary PHP versions should now be installed via Configuration → PHP Interperters.

Author Florian Cheno / as of: 1st of March 2024

HowTo – KeyHelp- Restic- Backup Restore

In the restore area, select the following elements:

- all email accounts
- all databases, **EXCEPT** for the ones already restored in point 2!
- all user folders `/home/users/` and `/var/spool/cron`
- **UNDER NO CIRCUMSTANCES** select `/etc` !

- restore `/root` later in another directory if necessary

- `/home/keyhelp` is not needed in normal cases – if Whitelabel is in use, restore the folder `/home/keyhelp/www/keyhelp.white_label`

Wait until the restore process is complete.

4) Restore SSL certificates

Change into the `/restore` folder and copy the certificates:

```
cd /restore
mv /etc/ssl/keyhelp /etc/ssl/keyhelp.bak
cp -av etc/ssl/keyhelp/ /etc/ssl/
rm -rf /etc/ssl/keyhelp.bak
```

5) Final operations

Rewrite the user configuration.

To do this, call up "`keyhelp-toolbox`" on the console -> select point 1 and follow the instructions of the script.

Reboot the server.

Done.

Author Florian Cheno / as of: 1st of March 2024