EPAM University Programs
DevOps external course
Module 4 Linux & Bash Essentials
TASK 4.7

Mariia Markina

Part1. **Quota allocation mechanism.**

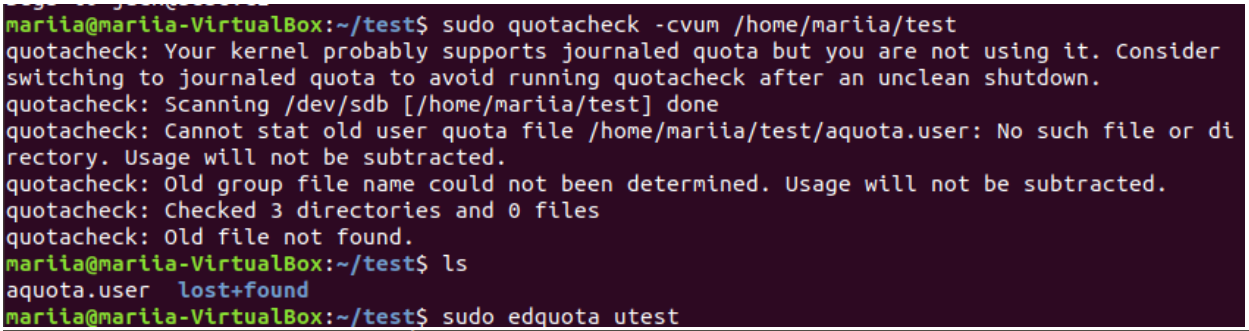
Employing commands from presentation #4.6, create a new user, say, *utest*. Based on the quota mechanism, limit the available disk space for this user to **soft**: 100M and hard: 150M.

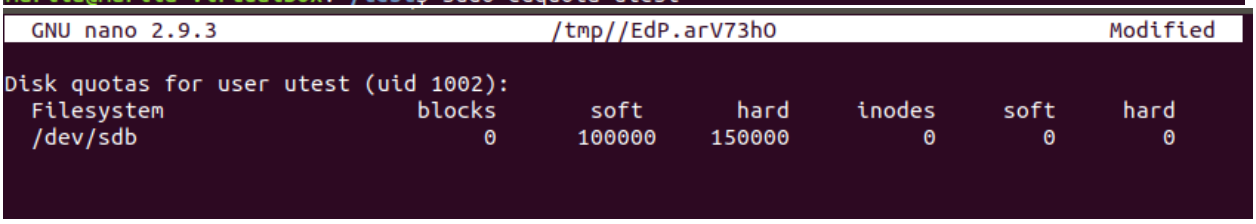
```
mariia@mariia-VirtualBox:~$ sudo groupadd newgroup
[sudo] password for mariia:
mariia@mariia-VirtualBox:~$ sudo useradd -g newgroup -s /bin/bash -d /home/
utest -m utest
```

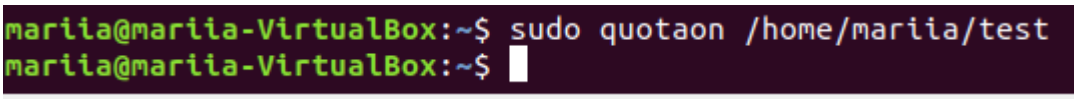
```
mariia@mariia-VirtualBox:~$ sudo apt install quota
[sudo] password for mariia:
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

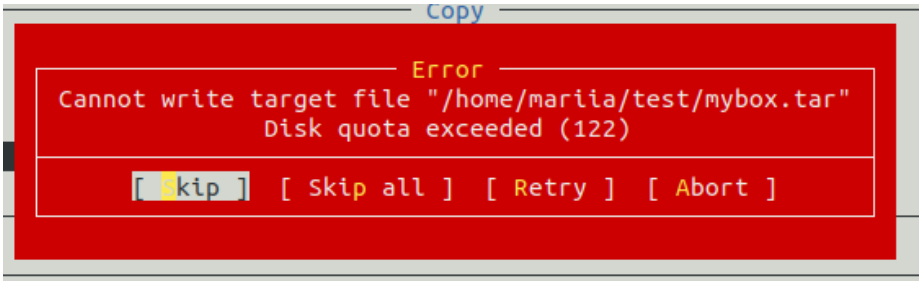
```
mariia@mariia-VirtualBox:~$ sudo mkfs.ext4 /dev/sdb
mke2fs 1.44.1 (24-Mar-2018)
Creating filesystem with 262144 4k blocks and 65536 inodes
Filesystem UUID: d73eafdd-36f4-454a-a925-4bdce5346bf6
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

ations
a@mariia-VirtualBox:~$ sudo mount /dev/sdb /home/mariia/test
```

```
  GNU nano 2.9.3

# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda1 during installation
UUID=3a501af9-4092-4167-a6f0-434e93950c8d /               ext4    errors=remount-ro 0       1
/swapfile                                 none            swap    sw              0       0
UUID=d73eafdd-36f4-454a-a925-4bdce5346bf6 /home/mariia/test ext4 defaults,userquota 0 0
```









Then, using Midnight Commander (since MC shows warnings about exceeding the limits of available to a user disk space), copy content of /usr directory to utest's home directory (actually, /usr isn't mandatory, you are free to copy any other data, the only condition is sufficient total size of the files to copy).

Note: if /home is not a mount point, then the **mount** and **quotaon** commands should be called with respect to the root partition /.

Note 2: Please, put into your report screenshots of your terminal window with the executed commands, along with screenshots of MC panels over which quota warnings are shown (i.e. warnings about exceeding soft and hard limits).

Part2. **Access Control Lists, ACLs**

In what follows, we assume that there are two users: *guest* (included into the list of sudoers) and *utest*. None of the users is the superuser (i.e. UIDs of the users differ from 0).

The most task: to allow user *utest* visit *guest*'s home directory.

```
guest@mariia-VirtualBox:/tmp$ setfacl -m u:utest:rwx /home/guest
guest@mariia-VirtualBox:/tmp$ su utest
Password:
utest@mariia-VirtualBox:/tmp$ cd ..
utest@mariia-VirtualBox:/$ cd /home
utest@mariia-VirtualBox:/home$ cd /guest
bash: cd: /guest: No such file or directory
utest@mariia-VirtualBox:/home$ ls
guest  mariia  user  utest
utest@mariia-VirtualBox:/home$ cd guest
utest@mariia-VirtualBox:/home/guest$ touch utest.txt
utest@mariia-VirtualBox:/home/guest$ ls -l
total 48
drwxr-xr-x 2 guest guest    4096 кві 24 15:36 Desktop
drwxr-xr-x 2 guest guest    4096 кві 24 15:36 Documents
drwxr-xr-x 2 guest guest    4096 кві 24 15:36 Downloads
-rw-r--r-- 1 guest guest    8980 кві 16  2018 examples.desktop
drwxr-xr-x 2 guest guest    4096 кві 24 15:36 Music
drwxr-xr-x 2 guest guest    4096 кві 24 15:36 Pictures
drwxr-xr-x 2 guest guest    4096 кві 24 15:36 Public
drwxr-xr-x 3 guest guest    4096 кві 24 15:36 snap
drwxr-xr-x 2 guest guest    4096 кві 24 15:36 Templates
-rw-r--r-- 1 utest newgroup    0 кві 24 17:27 utest.txt
```

The average task: to acquaint yourself with the basics of ACL and verify the fact that ACL privileges override the **chmod** ones.

Before proceeding to the task execution, please, visit the linux.org page describing ACL, https://linuxconfig.org/how-to-manage-acls-on-linux.

Every step of execution should be stored into some file **/var/log** directory (use logger, please).

1. Based on given in presentation #4.7 instructions, turn on and set up the ACL. *Caution*! The fact that a file system has been mounted with the “acl” flag on by default, doesn’t mean that the ACL package is installed.

Prior to any action, it is advised to check if the “acl” flag is on, using

tune2fs -l /dev/sda*

(a particular name of the device file sda*, is to be determined by calling to **blkid**, invoke it twice:

(i) on behalf of *guest* (i.e. without the superuser privileges);

(ii) with **sudo** (i.e. with the superuser privileges). Note the level of details provided by different **blkid** outputs).

```
guest@mariia-VirtualBox:~$ sudo tune2fs -l /dev/sda1 | logger -t homework
guest@mariia-VirtualBox:~$ sudo cat /var/log/syslog | grep "homework"
Apr 24 15:27:01 mariia-VirtualBox homework: checking logs
Apr 24 15:37:23 mariia-VirtualBox homework: Reading package lists...
Apr 24 15:37:24 mariia-VirtualBox homework: Building dependency tree...
Apr 24 15:37:24 mariia-VirtualBox homework: Reading state information...
Apr 24 15:37:26 mariia-VirtualBox homework: acl is already the newest version (2.2.52-3build1).
Apr 24 15:37:26 mariia-VirtualBox homework: acl set to manually installed.
Apr 24 15:37:26 mariia-VirtualBox homework: 0 upgraded, 0 newly installed, 0 to remove and 65 not upgraded.
Apr 24 15:43:34 mariia-VirtualBox homework: tune2fs 1.44.1 (24-Mar-2018)
Apr 24 15:43:45 mariia-VirtualBox homework: tune2fs 1.44.1 (24-Mar-2018)
Apr 24 15:43:45 mariia-VirtualBox homework: Filesystem volume name:   <none>
Apr 24 15:43:45 mariia-VirtualBox homework: Last mounted on:          /
Apr 24 15:43:45 mariia-VirtualBox homework: Filesystem UUID:          3a501af9-4092-4167-a6f0-434e93950c8d
Apr 24 15:43:45 mariia-VirtualBox homework: Filesystem magic number:  0xEF53
Apr 24 15:43:45 mariia-VirtualBox homework: Filesystem revision #:    1 (dynamic)
Apr 24 15:43:45 mariia-VirtualBox homework: Filesystem features:      has_journal ext_attr resize_inode dir_index
xtra_isize metadata_csum
Apr 24 15:43:45 mariia-VirtualBox homework: Filesystem flags:         signed_directory_hash
Apr 24 15:43:45 mariia-VirtualBox homework: Default mount options:    user_xattr acl
Apr 24 15:43:45 mariia-VirtualBox homework: Filesystem state:         clean
Apr 24 15:43:45 mariia-VirtualBox homework: Errors behavior:          Continue
Apr 24 15:43:45 mariia-VirtualBox homework: Filesystem OS type:       Linux
Apr 24 15:43:45 mariia-VirtualBox homework: Inode count:              655360
Apr 24 15:43:45 mariia-VirtualBox homework: Block count:              2620928
Apr 24 15:43:45 mariia-VirtualBox homework: Reserved block count:     131046
Apr 24 15:43:45 mariia-VirtualBox homework: Free blocks:              152806
Apr 24 15:43:45 mariia-VirtualBox homework: Free inodes:              428475
Apr 24 15:43:45 mariia-VirtualBox homework: First block:              0
Apr 24 15:43:45 mariia-VirtualBox homework: Block size:               4096
Apr 24 15:43:45 mariia-VirtualBox homework: Fragment size:            4096
Apr 24 15:43:45 mariia-VirtualBox homework: Group descriptor size:    64
Apr 24 15:43:45 mariia-VirtualBox homework: Reserved GDT blocks:      1024
Apr 24 15:43:45 mariia-VirtualBox homework: Blocks per group:         32768
Apr 24 15:43:45 mariia-VirtualBox homework: Fragments per group:      32768
Apr 24 15:43:45 mariia-VirtualBox homework: Inodes per group:         8192
Apr 24 15:43:45 mariia-VirtualBox homework: Inode blocks per group:   512
Apr 24 15:43:45 mariia-VirtualBox homework: Flex block group size:    16
Apr 24 15:43:45 mariia-VirtualBox homework: Filesystem created:       Tue Mar 24 16:55:23 2020
Apr 24 15:43:45 mariia-VirtualBox homework: Last mount time:          Fri Apr 24 15:32:22 2020
Apr 24 15:43:45 mariia-VirtualBox homework: Last write time:          Fri Apr 24 15:32:16 2020
```

2. Log in as *guest*. Create in */tmp* a directory called *acl_test*. By means of **chmod,** allow user utest to perform all possible operations (rwx) with respect to *acl_test.* Verify that user *utest* is indeed capable of implementing granted him (her) privileges. For example, acer logging in as *utest*, create a file in */tmp/acl_test*, say, *utest.txt* with the aid of **touch**. Query information about the directory and file by calling to

ls -ld /tmp/acl_test

ls -l /tmp/acl_test

```
guest@mariia-VirtualBox:/tmp$ mkdir acl_test
guest@mariia-VirtualBox:/tmp$ chmod 777 acl_test
utest@mariia-VirtualBox:/tmp$ cd acl_test
utest@mariia-VirtualBox:/tmp/acl_test$ touch utest.txt
utest@mariia-VirtualBox:/tmp/acl_test$ ls -ld /tmp/acl_test | logger -t homework
utest@mariia-VirtualBox:/tmp/acl_test$ ls -l /tmp/acl_test | logger -t homework
utest@mariia-VirtualBox:/tmp/acl_test$ getfacl /tmp/acl_test |logger -t homework
getfacl: Removing leading '/' from absolute path names
utest@mariia-VirtualBox:/tmp/acl_test$ getfacl /tmp/acl_test/utest.txt |logger -
t homework
getfacl: Removing leading '/' from absolute path names
```

To check ACL permissions do:

getfacl /tmp/acl_test

getfacl /tmp/acl_test/utest.txt

```
Apr 24 16:21:27 mariia-VirtualBox homework: total 36
Apr 24 16:21:27 mariia-VirtualBox homework: drwxrwxrwx 2 guest guest 4096 кві 24 16:19 acl_test
Apr 24 16:21:27 mariia-VirtualBox homework: -rw------- 1 guest guest    0 кві 24 16:19 config-err-NCZNVq
Apr 24 16:21:27 mariia-VirtualBox homework: drwx------ 3 root  root  4096 кві 24 16:10 snap.lxd
Apr 24 16:21:27 mariia-VirtualBox homework: drwx------ 2 guest guest 4096 кві 24 16:19 ssh-FXyZUIEQgMTq
Apr 24 16:21:27 mariia-VirtualBox homework: drwx------ 3 root  root  4096 кві 24 16:12 systemd-private-5e41530c265d4ea286d11cba952a6327-bolt.service-eZ1HbP
Apr 24 16:21:27 mariia-VirtualBox homework: drwx------ 3 root  root  4096 кві 24 16:12 systemd-private-5e41530c265d4ea286d11cba952a6327-colord.service-Raenzd
Apr 24 16:21:27 mariia-VirtualBox homework: drwx------ 3 root  root  4096 кві 24 16:20 systemd-private-5e41530c265d4ea286d11cba952a6327-fwupd.service-QpcMiC
Apr 24 16:21:27 mariia-VirtualBox homework: drwx------ 3 root  root  4096 кві 24 16:10 systemd-private-5e41530c265d4ea286d11cba952a6327-ModemManager.service-shW71a
Apr 24 16:21:27 mariia-VirtualBox homework: drwx------ 3 root  root  4096 кві 24 16:12 systemd-private-5e41530c265d4ea286d11cba952a6327-rtkit-daemon.service-CuwWP4
Apr 24 16:21:27 mariia-VirtualBox homework: drwx------ 3 root  root  4096 кві 24 16:10 systemd-private-5e41530c265d4ea286d11cba952a6327-systemd-resolved.service-3tLNbv
Apr 24 16:24:19 mariia-VirtualBox homework: drwxrwxrwx 2 guest guest 4096 кві 24 16:23 /tmp/acl_test
Apr 24 16:24:29 mariia-VirtualBox homework: total 0
Apr 24 16:24:29 mariia-VirtualBox homework: -rw-r--r-- 1 utest newgroup 0 кві 24 16:23 utest.txt
Apr 24 16:28:34 mariia-VirtualBox homework: # file: tmp/acl_test
Apr 24 16:28:34 mariia-VirtualBox homework: # owner: guest
Apr 24 16:28:34 mariia-VirtualBox homework: # group: guest
Apr 24 16:28:34 mariia-VirtualBox homework: user::rwx
Apr 24 16:28:34 mariia-VirtualBox homework: group::rwx
Apr 24 16:28:34 mariia-VirtualBox homework: other::rwx
Apr 24 16:28:34 mariia-VirtualBox homework:
Apr 24 16:28:51 mariia-VirtualBox homework: # file: tmp/acl_test/utest.txt
Apr 24 16:28:51 mariia-VirtualBox homework: # owner: utest
Apr 24 16:28:51 mariia-VirtualBox homework: # group: newgroup
Apr 24 16:28:51 mariia-VirtualBox homework: user::rw-
Apr 24 16:28:51 mariia-VirtualBox homework: group::r--
Apr 24 16:28:51 mariia-VirtualBox homework: other::r--
Apr 24 16:28:51 mariia-VirtualBox homework:
```

3. Employ ACL to block any activity except for reading, for user *utest* with respect to directory */tmp/acl_test* (hint: use **setfacl**). Test if the actions are effectively prohibited

```
guest@mariia-VirtualBox:/tmp/acl_test$ setfacl -m u:utest:r-- /tmp/acl_test
```

```
utest@mariia-VirtualBox:/tmp$ getfacl /tmp/acl_test
getfacl: Removing leading '/' from absolute path names
# file: tmp/acl_test
# owner: guest
# group: guest
user::rwx
user:utest:r--
group::rwx
mask::rwx
other::rwx
```

touch /tmp/acl_test/prohibited.txt

Is it possible to invoke this command?

echo “new content” > /tmp/acl_test/utest.txt

Test if user *utest* can be prevented from modifying content of the file *utest.txt* by means of ACL. (Note that user *utest* is the owner of the file *tmp/acl_test/utest.txt*).

No, ACL rules are stronger than that.

```
utest@mariia-VirtualBox:/tmp$ touch /tmp/acl_test/prohibited.txt | logger -t
homework
touch: cannot touch '/tmp/acl_test/prohibited.txt': Permission denied
utest@mariia-VirtualBox:/tmp$ echo "new content">/tmp/acl_test/utest.txt |log
ger -t homework
bash: /tmp/acl_test/utest.txt: Permission denied
utest@mariia-VirtualBox:/tmp$
```

4. Consider a situation when at the ACL level user *utest* is allowed to have all possible privileges with respect to */tmp/acl_test*, while no ac=on is allowed with **chmod** (conventional mechanism). (Hint: repeat step 3, but given the new context). *Again, ACL rules are stronger then chmod.*

```
guest@mariia-VirtualBox:/tmp$ sudo chmod  000  acl_test
guest@mariia-VirtualBox:/tmp$ setfacl -m u:utest:rwx /tmp/acl_test
```

```
utest@mariia-VirtualBox:/tmp$ touch /tmp/acl_test/prohibited.txt
|logger -t homework
utest@mariia-VirtualBox:/tmp$ echo "new content">/tmp/acl_test/ut
est.txt | logger -t homework
```

5. For user *utest*, set default ACLs to the directory */tmp/acl_test* which allow read-only access (hint: use the -d option of the **setfacl** command). Being logged in as *utest*, invoke **touch** to create the file *utest2.txt* in the */tmp/acl_test* directory. Query permissions on this file using **getfacl**.

```
guest@mariia-VirtualBox:/tmp$ setfacl -d -m u:utest:r-- /tmp/acl_test
guest@mariia-VirtualBox:/tmp$ su utest
Password:
utest@mariia-VirtualBox:/tmp$ touch /tmp/acl_test/utest2.txt
utest@mariia-VirtualBox:/tmp$ getfacl /tmp/acl_test/utest2.txt
getfacl: Removing leading '/' from absolute path names
# file: tmp/acl_test/utest2.txt
# owner: utest
# group: newgroup
user::---
user:utest:r--
group::rwx                      #effective:rw-
mask::rw-
other::---

utest@mariia-VirtualBox:/tmp$
```

6. Set the maximum permissions mask on the */tmp/acl_test/utest.txt* file in such a way as to allow read-only access. Check permissions with **getfacl**.

```
guest@mariia-VirtualBox:/tmp$ setfacl -m m::r /tmp/acl_test
guest@mariia-VirtualBox:/tmp$ getfacl /tmp/acl_test | logger -t homework
getfacl: Removing leading '/' from absolute path names
```

```
Apr 24 17:21:10 mariia-VirtualBox homework: group::rwx#011#effective:r--
Apr 24 17:21:10 mariia-VirtualBox homework: mask::r--
Apr 24 17:21:10 mariia-VirtualBox homework: other::---
Apr 24 17:21:10 mariia-VirtualBox homework: default:user::---
Apr 24 17:21:10 mariia-VirtualBox homework: default:user:utest:r--
Apr 24 17:21:10 mariia-VirtualBox homework: default:group::rwx
Apr 24 17:21:10 mariia-VirtualBox homework: default:mask::rwx
Apr 24 17:21:10 mariia-VirtualBox homework: default:other::---
Apr 24 17:21:10 mariia-VirtualBox homework:
```

7. Delete all ACL entries relative to the */tmp/acl_test* directory.

```
guest@mariia-VirtualBox:/tmp$ setfacl -b /tmp/acl_test
```