EPAM University Programs

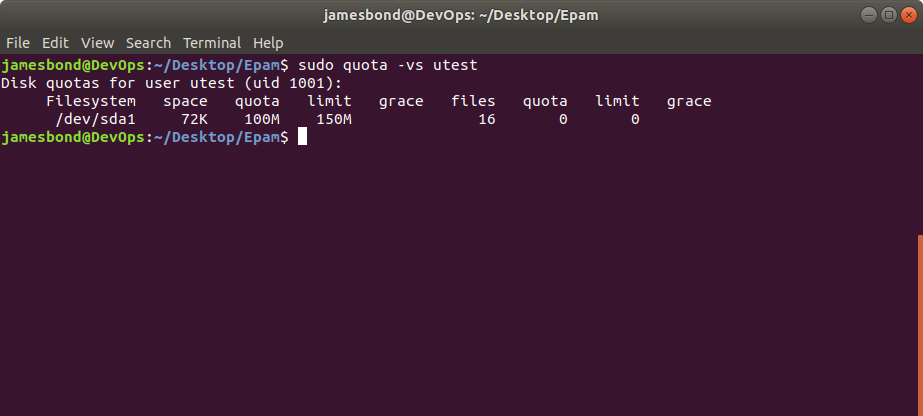
DevOps external course

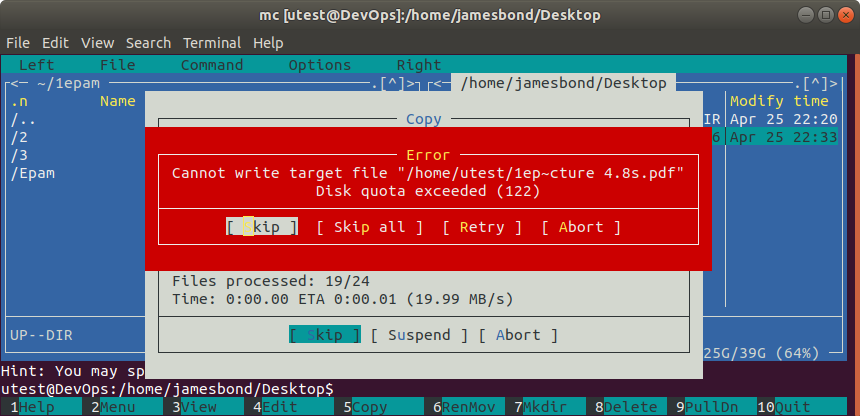
Module 4 Linux & Bash Essentials

TASK 4.7

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.





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**

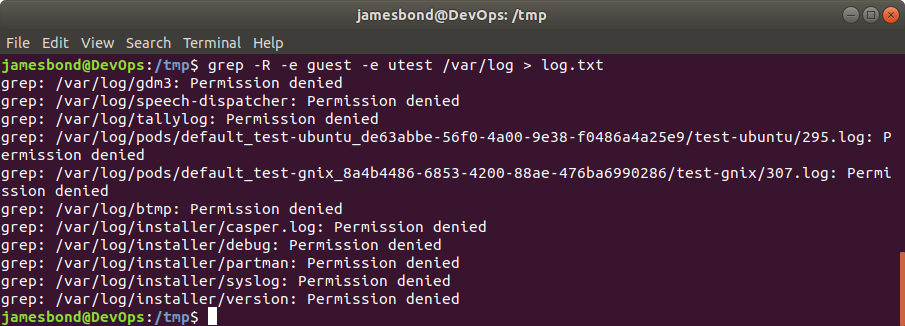
In what follows, we assume that there are two users: guest (included into the list of sudoers) and utest. None of the users is the superuser (i.e. UIDs of the users differ from 0).

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

**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).

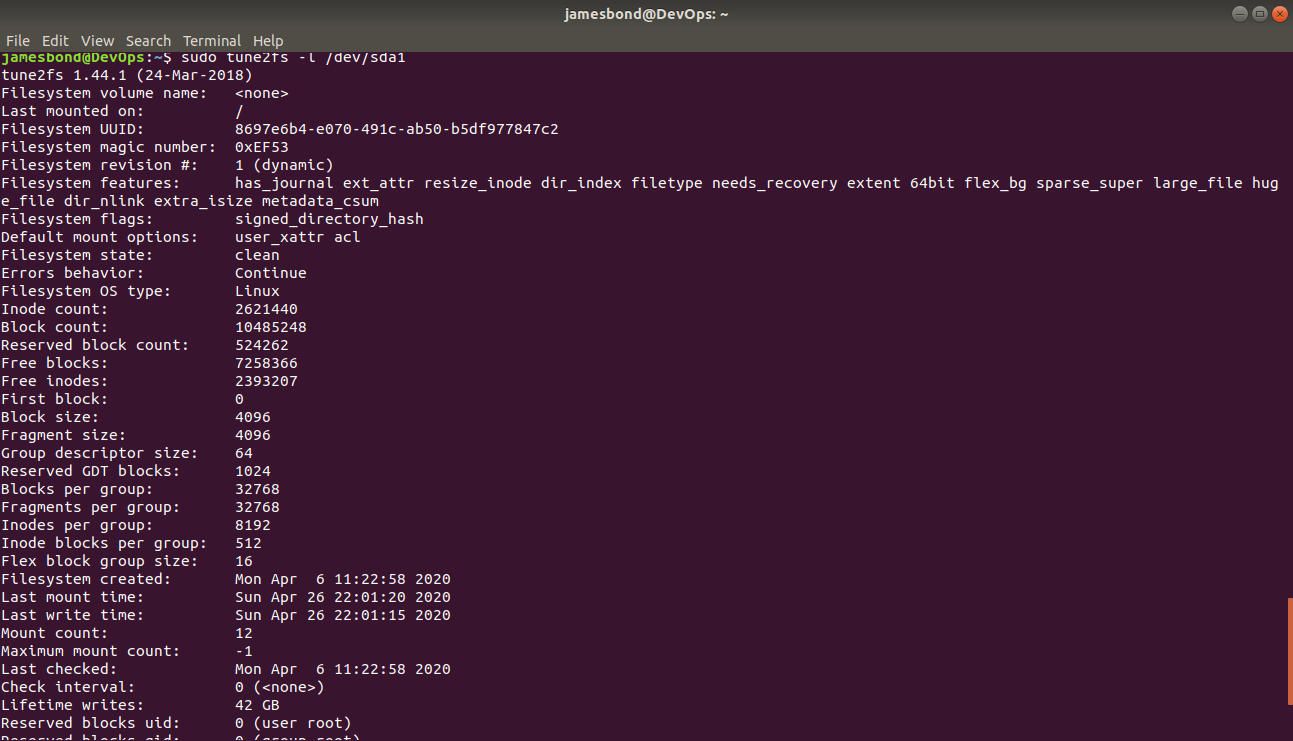


1. Based on given in presentation #4.7 instructions, turn on and set up the ACL. Caution! The fact that a file system has been mounted with the “acl” flag on by default, doesn’t mean that the ACL package is installed.

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

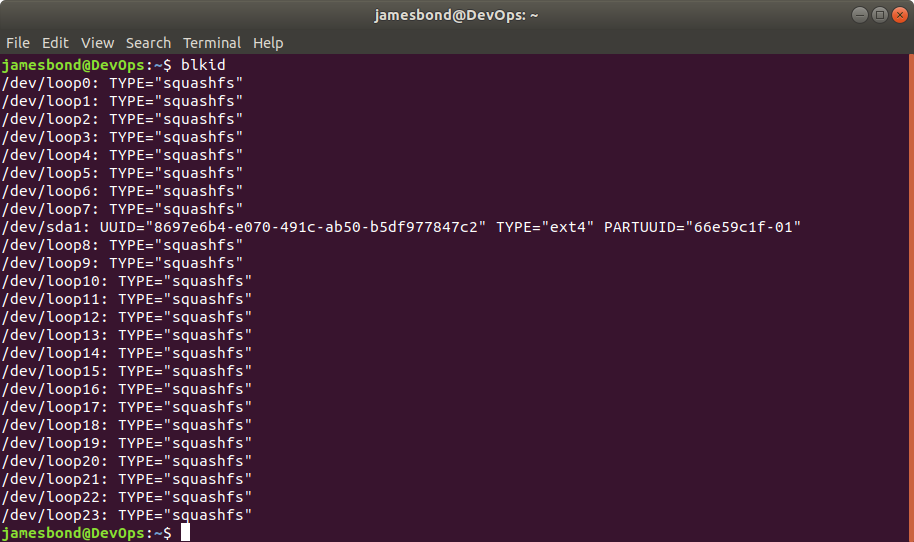
tune2fs -l /dev/sda\*

(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).



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

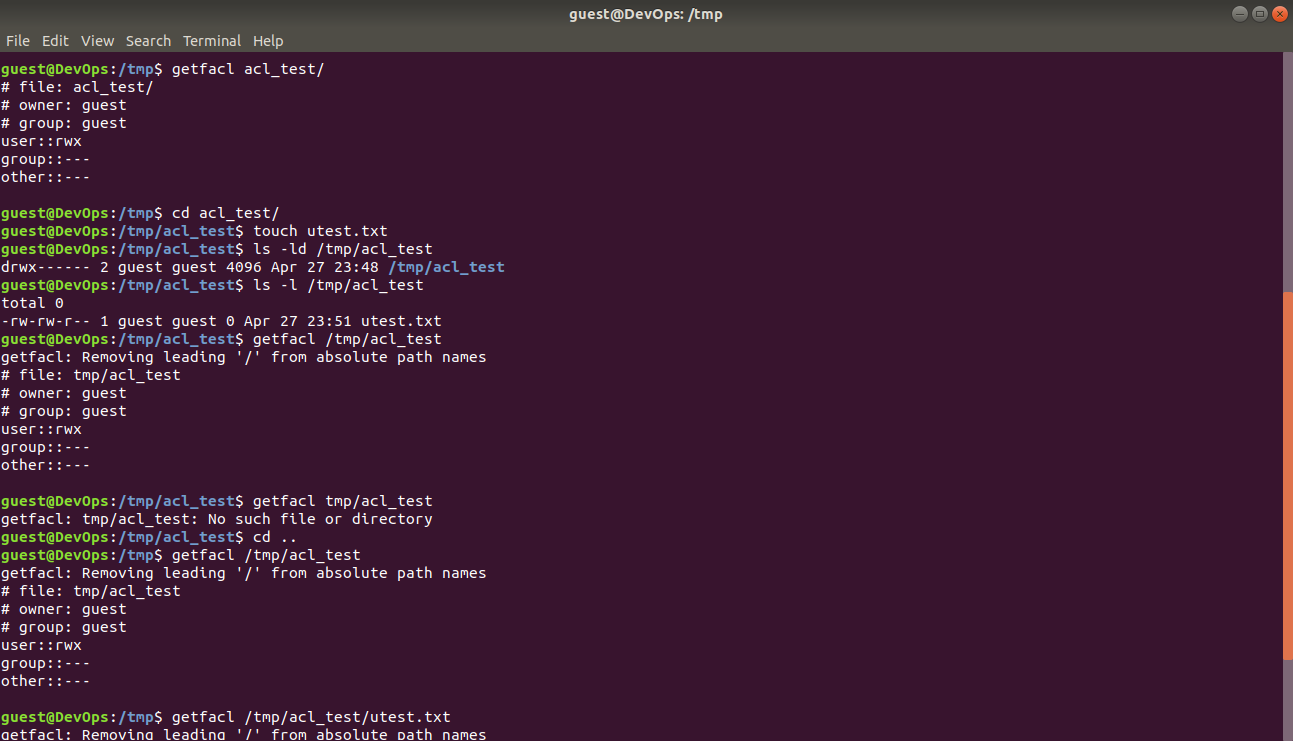
ls -ld /tmp/acl\_test

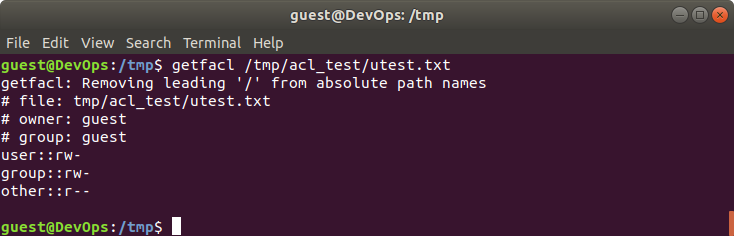
ls -l /tmp/acl\_test

To check ACL permissions do:

getfacl /tmp/acl\_test

getfacl /tmp/acl\_test/utest.txt





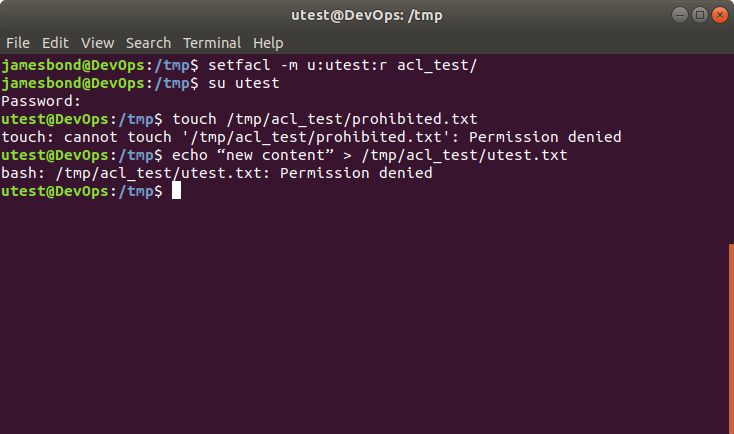
3. Employ ACL to block any activity except for reading, for user utest with respect to directory /tmp/acl\_test (hint: use setfacl). Test if the actions are effectively prohibited

touch /tmp/acl\_test/prohibited.txt

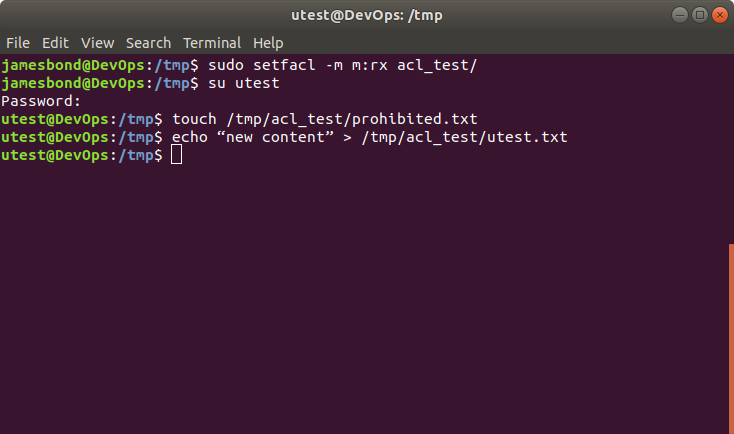
Is it possible to invoke this command?

echo “new content” > /tmp/acl\_test/utest.txt

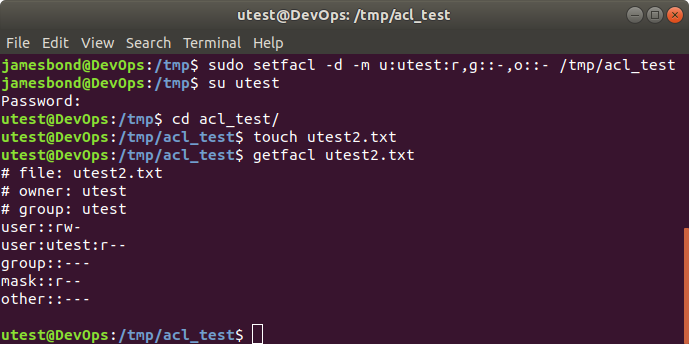
Test if user utest can be prevented from modifying content of the file utest.txt by means of ACL. (Note that user utest is the owner of the file tmp/acl\_test/utest.txt).



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 action is allowed with chmod (conventional mechanism). (Hint: repeat step 3, but given the new context).



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 directory. Query permissions on this file using getfacl.



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.



7. Delete all ACL entries relative to the /tmp/acl\_test directory.

