EPAM University Programs

DevOps external course

Module 4 Linux & Bash Essentials

TASK 4.7

Part1. **Quota allocation mechanism.**

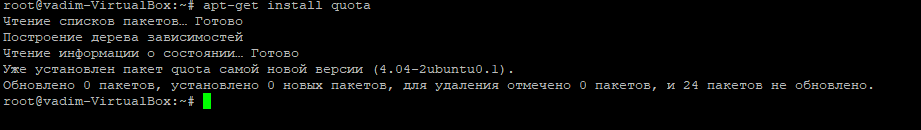
Employing commands from presentation #4.6, create a new user, say, utest. Based on the quota mechanism, limit the available disk space for this user to soft: 100M and hard: 150M.

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).

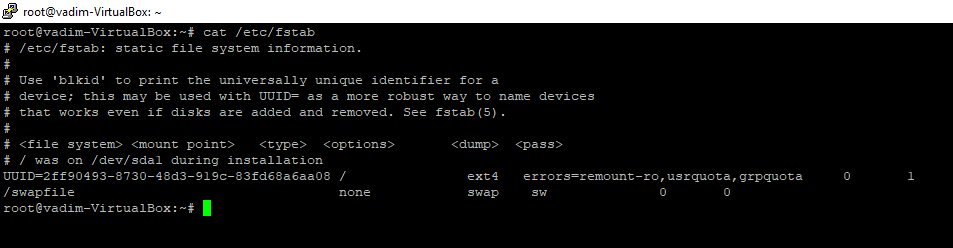
Note: if /home is not a mount point, then the mount and quotaon commands should be called with respect to the root partition /.

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).

1. Installing the Quota Tools



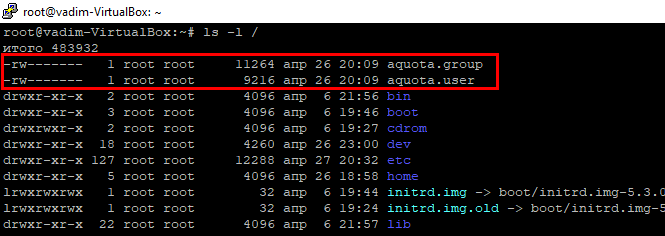
1. Updating Filesystem Mount Options



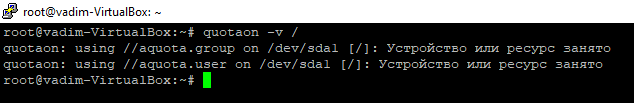
1. Enabling Quotas

# quotacheck –ugm /

ls –l /

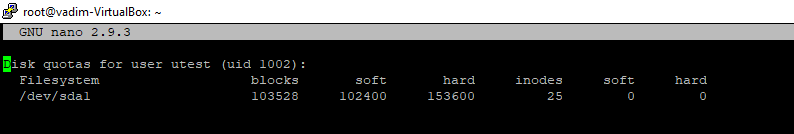


# quotaon -v /

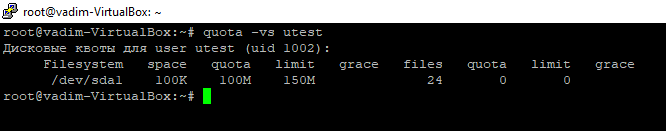


1. Configuring Quotas for a user ”utest”

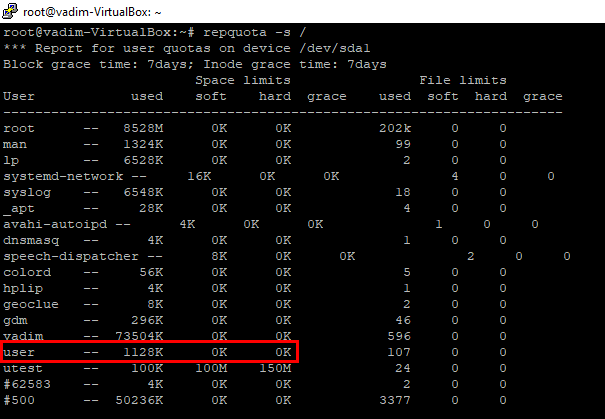
edquota –u utest



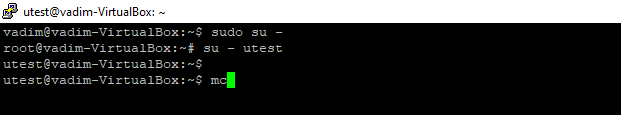
To check the quota enabled of username “utest”

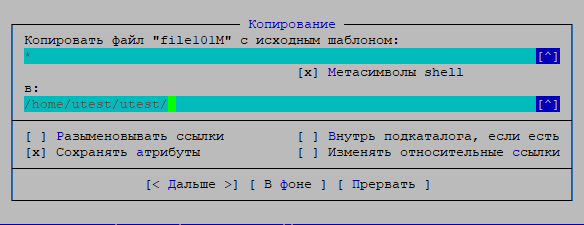


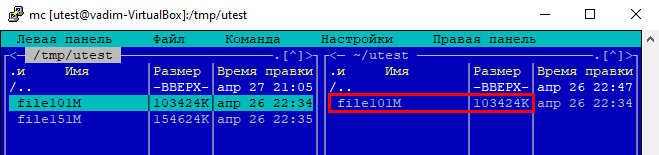
1. Generating the quota reports of all users

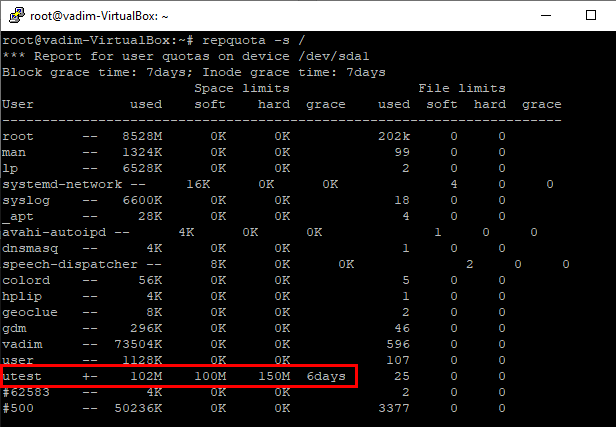


1. Testing how the quota is work, copy file of size 101M in utest’s $HOMEDIR

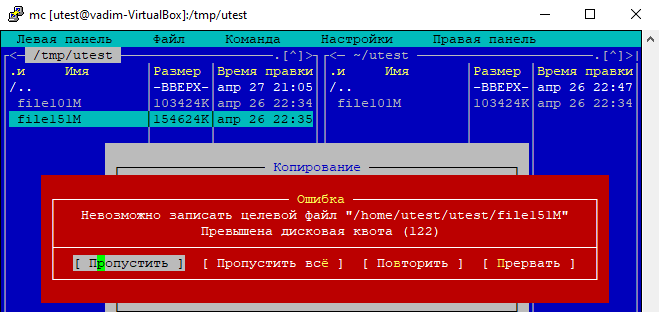


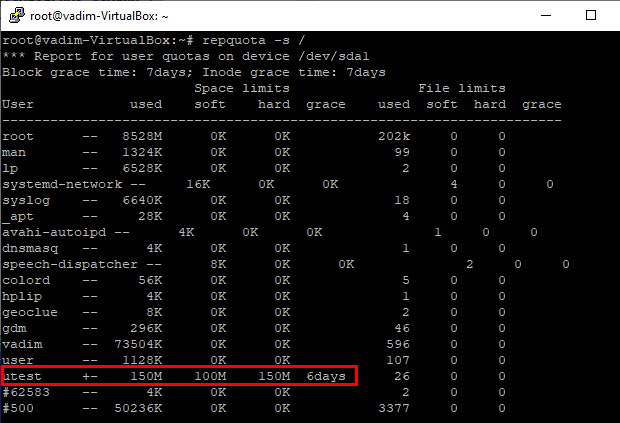






Copy file of size 151M in utest’s $HOMEDIR





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:

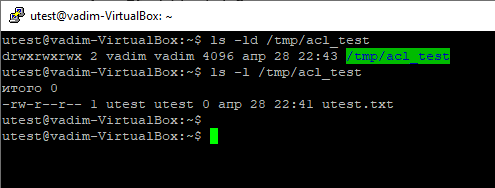
(i) on behalf of guest (i.e. without the superuser privileges);

(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

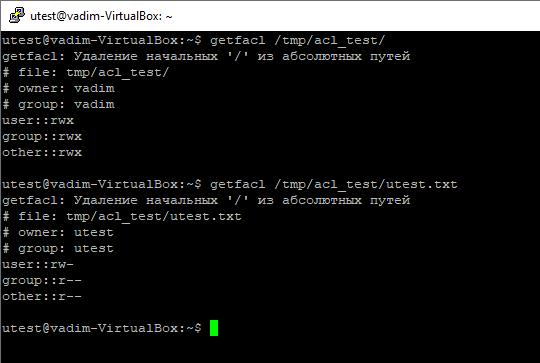
ls -l /tmp/acl\_test



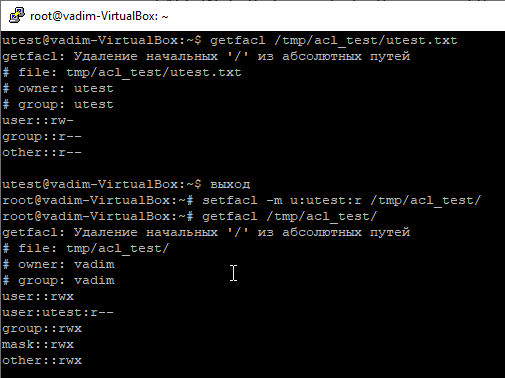
To check ACL permissions do:

ge4acl /tmp/acl\_test

ge4acl /tmp/acl\_test/utest.txt

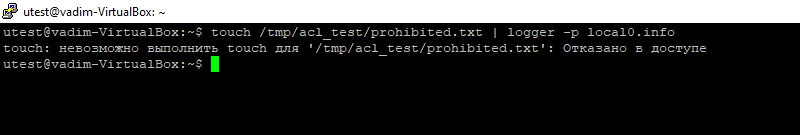


3. Employ ACL to block any activity except for reading, for user utest with respect to directory /tmp/acl\_test (hint: use se4acl). Test if the actions are effectively prohibited

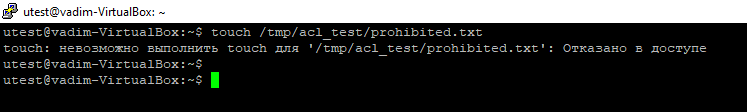


touch /tmp/acl\_test/prohibited.txt

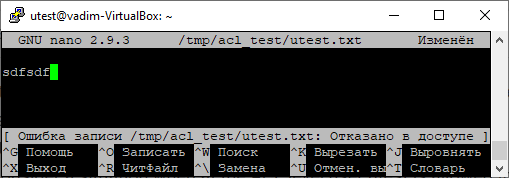
Is it possible to invoke this command?



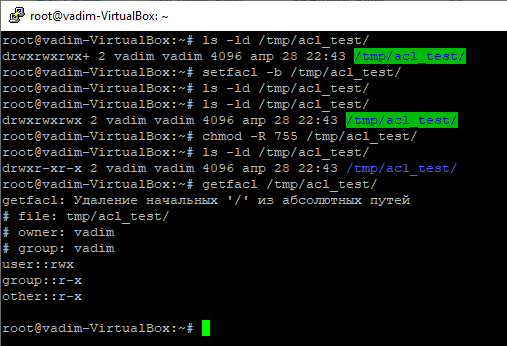
echo “new content” > /tmp/acl\_test/utest.txt



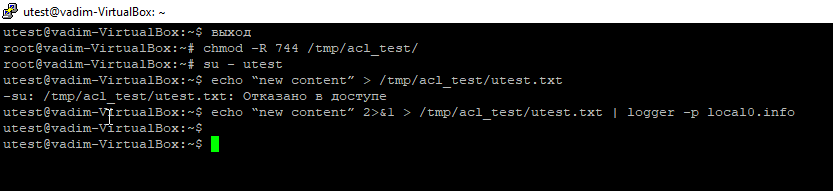
Test if user utest can be prevented from modifying content of the file utest.txt by means of ACL. (Note that user utest is the owner of the file tmp/acl\_test/utest.txt).



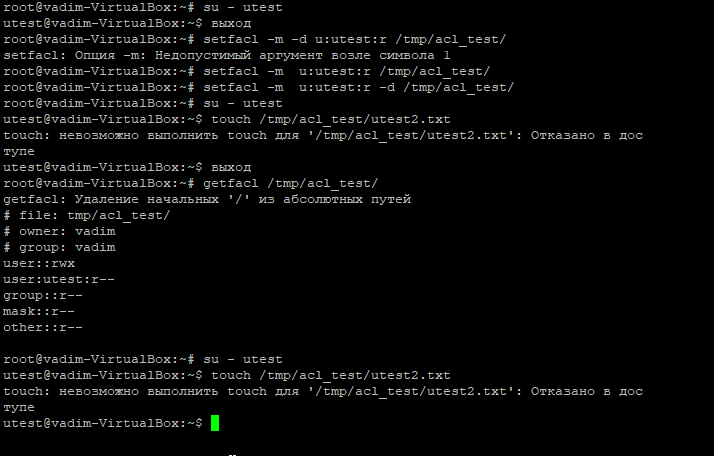
4. Consider a situation when at the ACL level user utest is allowed to have all possible privileges with respect to /tmp/acl\_test, while no ac=on is allowed with chmod (conventional mechanism). (Hint: repeat step 3, but given the new context).



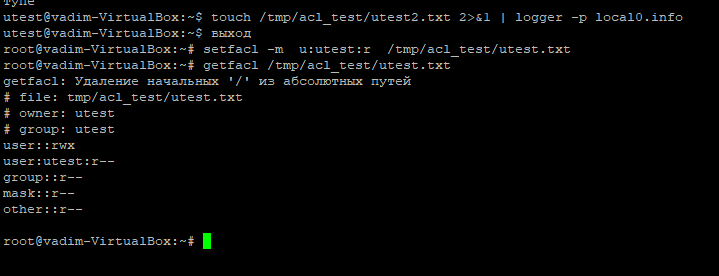
When we use the rights 744 of directory **/tmp/acl\_test/**



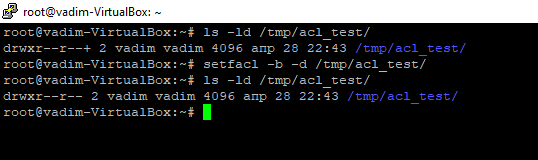
5. For user utest, set default ACLs to the directory /tmp/acl\_test which allow read-only access (hint: use the -d option of the se4acl command). Being logged in as utest, invoke touch to create the file utest2.txt in the /tmp/acl\_test directory. Query permissions on this file using ge4acl.

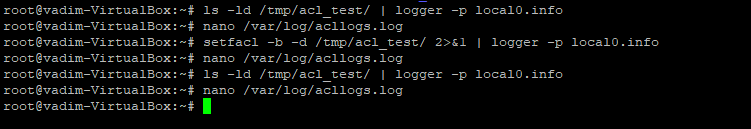


6. Set the maximum permissions mask on the /tmp/acl\_test/utest.txt file in such a way as to allow read-only access. Check permissions with ge4acl.

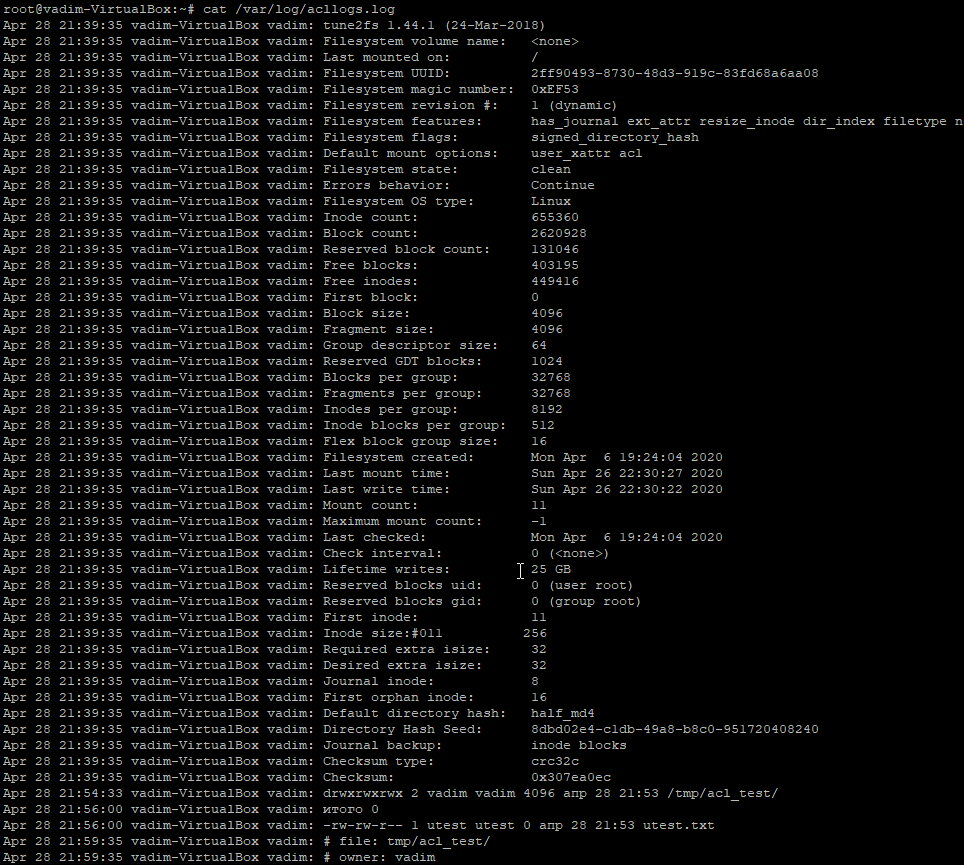


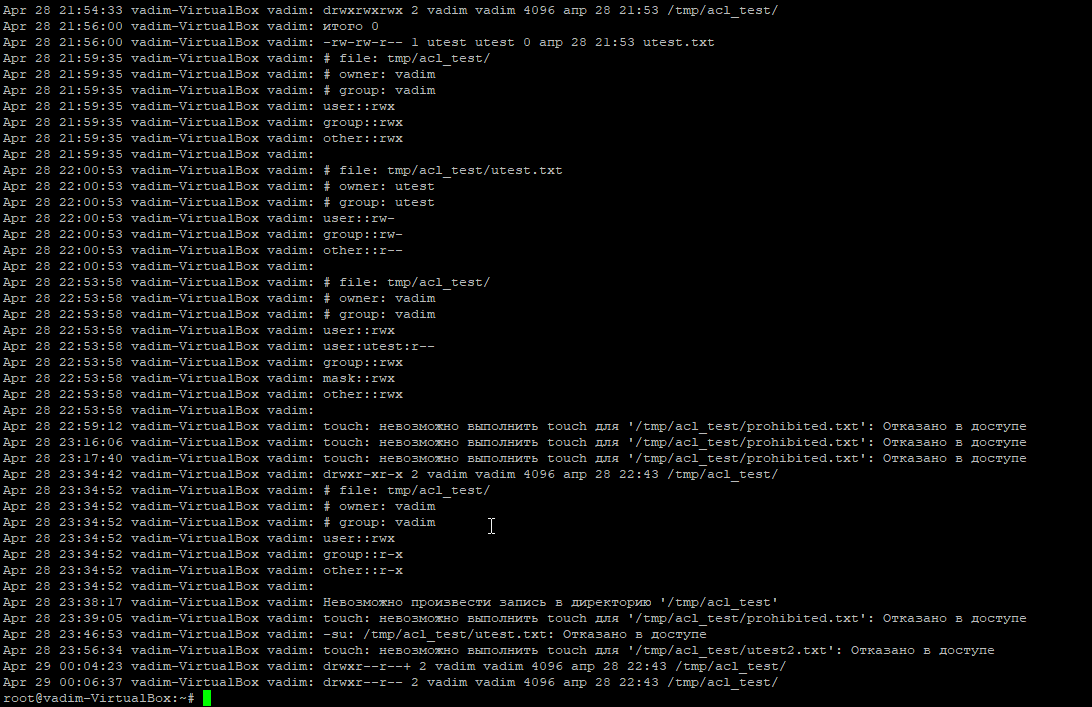
7. Delete all ACL entries relative to the /tmp/acl\_test directory.





Listing log file /var/log/acllogs.log





root@vadim-VirtualBox:~# cat /var/log/acllogs.log

Apr 28 21:39:35 vadim-VirtualBox vadim: tune2fs 1.44.1 (24-Mar-2018)

Apr 28 21:39:35 vadim-VirtualBox vadim: Filesystem volume name: <none>

Apr 28 21:39:35 vadim-VirtualBox vadim: Last mounted on: /

Apr 28 21:39:35 vadim-VirtualBox vadim: Filesystem UUID: 2ff90493-8730-48d3-919c-83fd68a6aa08

Apr 28 21:39:35 vadim-VirtualBox vadim: Filesystem magic number: 0xEF53

Apr 28 21:39:35 vadim-VirtualBox vadim: Filesystem revision #: 1 (dynamic)

Apr 28 21:39:35 vadim-VirtualBox vadim: Filesystem features: has\_journal ext\_attr resize\_inode dir\_index filetype needs\_recovery extent 64bit flex\_bg sparse\_super large\_file huge\_file dir\_nlink extra\_isize metadata\_csum

Apr 28 21:39:35 vadim-VirtualBox vadim: Filesystem flags: signed\_directory\_hash

Apr 28 21:39:35 vadim-VirtualBox vadim: Default mount options: user\_xattr acl

Apr 28 21:39:35 vadim-VirtualBox vadim: Filesystem state: clean

Apr 28 21:39:35 vadim-VirtualBox vadim: Errors behavior: Continue

Apr 28 21:39:35 vadim-VirtualBox vadim: Filesystem OS type: Linux

Apr 28 21:39:35 vadim-VirtualBox vadim: Inode count: 655360

Apr 28 21:39:35 vadim-VirtualBox vadim: Block count: 2620928

Apr 28 21:39:35 vadim-VirtualBox vadim: Reserved block count: 131046

Apr 28 21:39:35 vadim-VirtualBox vadim: Free blocks: 403195

Apr 28 21:39:35 vadim-VirtualBox vadim: Free inodes: 449416

Apr 28 21:39:35 vadim-VirtualBox vadim: First block: 0

Apr 28 21:39:35 vadim-VirtualBox vadim: Block size: 4096

Apr 28 21:39:35 vadim-VirtualBox vadim: Fragment size: 4096

Apr 28 21:39:35 vadim-VirtualBox vadim: Group descriptor size: 64

Apr 28 21:39:35 vadim-VirtualBox vadim: Reserved GDT blocks: 1024

Apr 28 21:39:35 vadim-VirtualBox vadim: Blocks per group: 32768

Apr 28 21:39:35 vadim-VirtualBox vadim: Fragments per group: 32768

Apr 28 21:39:35 vadim-VirtualBox vadim: Inodes per group: 8192

Apr 28 21:39:35 vadim-VirtualBox vadim: Inode blocks per group: 512

Apr 28 21:39:35 vadim-VirtualBox vadim: Flex block group size: 16

Apr 28 21:39:35 vadim-VirtualBox vadim: Filesystem created: Mon Apr 6 19:24:04 2020

Apr 28 21:39:35 vadim-VirtualBox vadim: Last mount time: Sun Apr 26 22:30:27 2020

Apr 28 21:39:35 vadim-VirtualBox vadim: Last write time: Sun Apr 26 22:30:22 2020

Apr 28 21:39:35 vadim-VirtualBox vadim: Mount count: 11

Apr 28 21:39:35 vadim-VirtualBox vadim: Maximum mount count: -1

Apr 28 21:39:35 vadim-VirtualBox vadim: Last checked: Mon Apr 6 19:24:04 2020

Apr 28 21:39:35 vadim-VirtualBox vadim: Check interval: 0 (<none>)

Apr 28 21:39:35 vadim-VirtualBox vadim: Lifetime writes: 25 GB

Apr 28 21:39:35 vadim-VirtualBox vadim: Reserved blocks uid: 0 (user root)

Apr 28 21:39:35 vadim-VirtualBox vadim: Reserved blocks gid: 0 (group root)

Apr 28 21:39:35 vadim-VirtualBox vadim: First inode: 11

Apr 28 21:39:35 vadim-VirtualBox vadim: Inode size:#011 256

Apr 28 21:39:35 vadim-VirtualBox vadim: Required extra isize: 32

Apr 28 21:39:35 vadim-VirtualBox vadim: Desired extra isize: 32

Apr 28 21:39:35 vadim-VirtualBox vadim: Journal inode: 8

Apr 28 21:39:35 vadim-VirtualBox vadim: First orphan inode: 16

Apr 28 21:39:35 vadim-VirtualBox vadim: Default directory hash: half\_md4

Apr 28 21:39:35 vadim-VirtualBox vadim: Directory Hash Seed: 8dbd02e4-c1db-49a8-b8c0-951720408240

Apr 28 21:39:35 vadim-VirtualBox vadim: Journal backup: inode blocks

Apr 28 21:39:35 vadim-VirtualBox vadim: Checksum type: crc32c

Apr 28 21:39:35 vadim-VirtualBox vadim: Checksum: 0x307ea0ec

Apr 28 21:54:33 vadim-VirtualBox vadim: drwxrwxrwx 2 vadim vadim 4096 апр 28 21:53 /tmp/acl\_test/

Apr 28 21:56:00 vadim-VirtualBox vadim: итого 0

Apr 28 21:56:00 vadim-VirtualBox vadim: -rw-rw-r-- 1 utest utest 0 апр 28 21:53 utest.txt

Apr 28 21:59:35 vadim-VirtualBox vadim: # file: tmp/acl\_test/

Apr 28 21:59:35 vadim-VirtualBox vadim: # owner: vadim

Apr 28 21:59:35 vadim-VirtualBox vadim: # group: vadim

Apr 28 21:59:35 vadim-VirtualBox vadim: user::rwx

Apr 28 21:59:35 vadim-VirtualBox vadim: group::rwx

Apr 28 21:59:35 vadim-VirtualBox vadim: other::rwx

Apr 28 21:59:35 vadim-VirtualBox vadim:

Apr 28 22:00:53 vadim-VirtualBox vadim: # file: tmp/acl\_test/utest.txt

Apr 28 22:00:53 vadim-VirtualBox vadim: # owner: utest

Apr 28 22:00:53 vadim-VirtualBox vadim: # group: utest

Apr 28 22:00:53 vadim-VirtualBox vadim: user::rw-

Apr 28 22:00:53 vadim-VirtualBox vadim: group::rw-

Apr 28 22:00:53 vadim-VirtualBox vadim: other::r--

Apr 28 22:00:53 vadim-VirtualBox vadim:

Apr 28 22:53:58 vadim-VirtualBox vadim: # file: tmp/acl\_test/

Apr 28 22:53:58 vadim-VirtualBox vadim: # owner: vadim

Apr 28 22:53:58 vadim-VirtualBox vadim: # group: vadim

Apr 28 22:53:58 vadim-VirtualBox vadim: user::rwx

Apr 28 22:53:58 vadim-VirtualBox vadim: user:utest:r--

Apr 28 22:53:58 vadim-VirtualBox vadim: group::rwx

Apr 28 22:53:58 vadim-VirtualBox vadim: mask::rwx

Apr 28 22:53:58 vadim-VirtualBox vadim: other::rwx

Apr 28 22:53:58 vadim-VirtualBox vadim:

Apr 28 22:59:12 vadim-VirtualBox vadim: touch: невозможно выполнить touch для '/tmp/acl\_test/prohibited.txt': Отказано в доступе

Apr 28 23:16:06 vadim-VirtualBox vadim: touch: невозможно выполнить touch для '/tmp/acl\_test/prohibited.txt': Отказано в доступе

Apr 28 23:17:40 vadim-VirtualBox vadim: touch: невозможно выполнить touch для '/tmp/acl\_test/prohibited.txt': Отказано в доступе

Apr 28 23:34:42 vadim-VirtualBox vadim: drwxr-xr-x 2 vadim vadim 4096 апр 28 22:43 /tmp/acl\_test/

Apr 28 23:34:52 vadim-VirtualBox vadim: # file: tmp/acl\_test/

Apr 28 23:34:52 vadim-VirtualBox vadim: # owner: vadim

Apr 28 23:34:52 vadim-VirtualBox vadim: # group: vadim

Apr 28 23:34:52 vadim-VirtualBox vadim: user::rwx

Apr 28 23:34:52 vadim-VirtualBox vadim: group::r-x

Apr 28 23:34:52 vadim-VirtualBox vadim: other::r-x

Apr 28 23:34:52 vadim-VirtualBox vadim:

Apr 28 23:38:17 vadim-VirtualBox vadim: Невозможно произвести запись в директорию '/tmp/acl\_test'

Apr 28 23:39:05 vadim-VirtualBox vadim: touch: невозможно выполнить touch для '/tmp/acl\_test/prohibited.txt': Отказано в доступе

Apr 28 23:46:53 vadim-VirtualBox vadim: -su: /tmp/acl\_test/utest.txt: Отказано в доступе

Apr 28 23:56:34 vadim-VirtualBox vadim: touch: невозможно выполнить touch для '/tmp/acl\_test/utest2.txt': Отказано в доступе

Apr 29 00:04:23 vadim-VirtualBox vadim: drwxr--r--+ 2 vadim vadim 4096 апр 28 22:43 /tmp/acl\_test/

Apr 29 00:06:37 vadim-VirtualBox vadim: drwxr--r-- 2 vadim vadim 4096 апр 28 22:43 /tmp/acl\_test/

root@vadim-VirtualBox:~#