/var/log/auth.log .:

/var/log/auth.log

```
Feb 19 12:32:48 nd-nout fly-dm: :0[3421]: pam_unix(fly-dm:session): session opened for user ivanov by (uid=0)
```

«ivanov».

/var/log/auth.log

```
Feb 19 13:15:38 ac-old login[3865]: pam_unix(login:session): session closed for user petrovich
```

«petrovich».

, parsec: /var/log/parsec/user.mlog, «userlog». «auth» (), «exit» ().

:

ac-old:~# userlog

```
[u] 'Tue Feb 19 12:50:00 2013' '/bin/login' <26828,26778,0,2500,0>[s] exit("login","petrovich")
[u] 'Tue Feb 19 12:57:59 2013' '/usr/bin/fly-dm' <25927,3462,0,0,0> [s] exit("fly-dm","root")
[u] 'Tue Feb 19 13:14:52 2013' '/bin/login' <3796,3680,0,0,0> [s] auth("login","root")
[u] 'Tue Feb 19 13:15:33 2013' '/bin/login' <3865,3683,0,2500,0> [s] auth("login","petrovich")
[u] 'Tue Feb 19 13:15:39 2013' '/bin/login' <3865,3683,0,2500,0> [s] exit("login","petrovich")
[u] 'Tue Feb 19 13:19:53 2013' '/bin/login' <3992,3898,0,2500,0> [s] auth("login","petrovich")
[u] 'Tue Feb 19 13:20:13 2013' '/bin/login' <3992,3898,0,2500,0> [s] exit("login","petrovich")
[u] 'Tue Feb 19 13:20:23 2013' '/bin/login' <4070,4020,0,2500,0> [s] auth("login","petrovich")
[u] 'Tue Feb 19 13:20:31 2013' '/bin/login' <4070,4020,0,2500,0> [s] exit("login","petrovich")
[u] 'Tue Feb 19 13:27:48 2013' '/bin/login' <4212,4091,0,2500,0> [s] auth("login","petrovich")
[u] 'Tue Feb 19 13:27:54 2013' '/bin/login' <4212,4091,0,2500,0> [s] exit("login","petrovich")
[u] 'Tue Feb 19 13:33:51 2013' '/bin/login' <4327,4234,0,2500,0> [s] auth("login","petrovich")
[u] 'Tue Feb 19 13:33:55 2013' '/bin/login' <4327,4234,0,2500,0> [s] exit("login","petrovich")
[u] 'Tue Feb 19 13:39:49 2013' '/bin/login' <4440,4348,0,2500,0> [s] auth("login","petrovich")
[u] 'Tue Feb 19 13:39:53 2013' '/bin/login' <4440,4348,0,2500,0> [s] exit("login","petrovich")
```

10 « «Astra Linux Special Edition». . 1». «man» , «man parselog». «Astra Linux Special Edition» « . . . » , . : () :

ac-old:~# ald-admin user-aud-get petrovich

```
Audit policy user:petrovich
Audit success rules: ocxudntligarmphew
nr f flag
-- - ----
0 o open
```

1 c create

2 x exec

3 u delete

4 d chmod

5 n chown

6 t mount

7 l module

8 i uid

9 g gid

10 a audit

11 r acl

12 m mac

13 p cap

14 h chroot

15 e rename

16 w net

Audit fail rules: ocxudntligarmphew

nr f flag

-- - ----

0 o open

1 c create

2 x exec

3 u delete

4 d chmod

5 n chown

6 t mount

7 l module

8 i uid

9 g gid

10 a audit

11 r acl

12 m mac

13 p cap

14 h chroot

15 e rename

16 w net

:

```
> /var/log/parsec/kernel.mlog
```

«petrovich». kernlog «petrovich»:

ac-old:~# kernlog | grep "petrovich*"

```
[p] 'Tue Feb 19 13:39:49 2013' '/bin/bash' <4450,4440,2500,2500,2500> [f] open("/ald_home/petrovich/.
bash_profile",O_RDONLY) = -2 ENOENT (    )

[p] 'Tue Feb 19 13:39:49 2013' '/bin/bash' <4450,4440,2500,2500,2500> [f] open("/ald_home/petrovich/.
bash_login",O_RDONLY) = -2 ENOENT (     )

[p] 'Tue Feb 19 13:39:49 2013' '/bin/bash' <4450,4440,2500,2500,2500> [f] open("/ald_home/petrovich/.profile",
O_RDONLY) = -2 ENOENT (     )

[p] 'Tue Feb 19 13:39:49 2013' '/bin/bash' <4450,4440,2500,2500,2500> [s] open("/ald_home/petrovich/.
bash_history",O_RDONLY) = 3

[p] 'Tue Feb 19 13:39:49 2013' '/bin/bash' <4450,4440,2500,2500,2500> [s] open("/ald_home/petrovich/.
bash_history",O_RDONLY) = 3

[p] 'Tue Feb 19 13:39:52 2013' '/bin/bash' <4450,4440,2500,2500,2500> [f] open("/ald_home/petrovich/.
bash_logout",O_RDONLY) = -2 ENOENT (     )

[p] 'Tue Feb 19 13:39:52 2013' '/bin/bash' <4450,4440,2500,2500,2500> [s] open("/ald_home/petrovich/.
bash_history",O_WRONLY | O_APPEND) = 3

[p] 'Tue Feb 19 13:39:52 2013' '/bin/bash' <4450,4440,2500,2500,2500> [s] open("/ald_home/petrovich/.
bash_history",O_RDONLY) = 3

[p] 'Tue Feb 19 13:39:52 2013' '/bin/login' <4440,4348,0,2500,0> [s] umount("/ald_home/petrovich/mac/0/0") = 0

[p] 'Tue Feb 19 13:39:52 2013' '/bin/login' <4440,4348,0,2500,0> [s] umount("/ald_home/petrovich/mac") = 0

[p] 'Tue Feb 19 13:39:52 2013' '/bin/login' <4440,4348,0,2500,0> [s] umount("/ald_home/petrovich") = 0

[p] 'Tue Feb 19 13:39:52 2013' '/bin/login' <4440,4348,0,2500,0> [s] umount("/var/private/mac/petrovich/0/0") =
0

[p] 'Tue Feb 19 13:39:52 2013' '/bin/login' <4440,4348,0,2500,0> [s] umount("/var/private/mac/petrovich") = 0

[p] 'Tue Feb 19 13:39:52 2013' '/usr/sbin/pmvarrun' <4453,4440,0,2500,0> [s] create("/var/run/pam_mount
/petrovich",O_RDWR | O_CREAT,-rw-------) = 7

[p] 'Tue Feb 19 13:39:52 2013' '/usr/sbin/pmvarrun' <4453,4440,0,2500,0> [s] chown("/var/run/pam_mount
/petrovich",2500,0) = 0

[p] 'Tue Feb 19 13:39:53 2013' '/sbin/umount.cifs' <4455,4454,0,2500,0> [s] umount("/ald_home/petrovich") = 0
```

«open» ( ), «mount» ( ), «create» ( ), «chown» ( ). «petrovich» «testdir» «testfile». — :

dc-old:~# ls -l /ald_export_home/petrovich/ | grep test

```
drwxr-x--- 2 petrovich petrovich 4096  19 13:50 testdir
```

dc-old:~# ls -l /ald_export_home/petrovich/testdir/

```
 4

-rwxr----- 1 petrovich petrovich 5  19 13:50 testfile
```

:

dc-old:/ald_export_home/petrovich# getfaud testdir/

```
# file: testdir

o:ouc:ouc

default:o:ouc:ouc
```

dc-old:/ald_export_home/petrovich# getfaud testdir/testfile

```
# file: testdir/testfile

o:ouc:ouc
```

«petrovich» testdir/testfile, testdir/testfile2. /var/log/parsec/kern.mlog :

kernlog

:

[f] 'Tue Feb 19 14:07:23 2013' '/usr/sbin/smbd' <6514,3024,0,0,2500> [s] open("/ald_export_home/petrovich/testdir",NO_PERMS | O_NONBLOCK | O_DIRECTORY) = 0

:

[f] 'Tue Feb 19 14:07:25 2013' '/usr/sbin/smbd' <6514,3024,0,0,2500> [s] unlink("/ald_export_home/petrovich/testdir/testfile (deleted)") = 0

:

[f] 'Tue Feb 19 14:07:34 2013' '/usr/sbin/smbd' <6514,3024,0,0,2500> [s] create("/ald_export_home/petrovich/testdir/testfile2",-rw-r-----) = 0

[f] 'Tue Feb 19 14:07:34 2013' '/usr/sbin/smbd' <6514,3024,0,0,2500> [s] open("/ald_export_home/petrovich/testdir/testfile2",O_RDONLY | O_CREAT | O_NOFOLLOW) = 0

:

[f] 'Tue Feb 19 14:12:15 2013' '/usr/bin/scp' <6609,6606,0,0,0> [s] create("/ald_export_home/petrovich/testdir/remote_cp",-rw-r--r--) = 0

[f] 'Tue Feb 19 14:12:15 2013' '/usr/bin/scp' <6609,6606,0,0,0> [s] open("/ald_export_home/petrovich/testdir/remote_cp",O_RDONLY | O_CREAT) = 0

, («create»), . / «chmac» ( ).

```
setfaud -s o:ocum:ocum testdir/testfile2

> /var/log/parsec/kernel.mlog

chmac 1:0 testdir/testfile2
```

dc-old:~# kernlog

[f] 'Tue Feb 19 14:24:55 2013' '/bin/bash' <5891,5887,0,0,0> [s] open("/ald_export_home/petrovich/testdir",NO_PERMS | O_NONBLOCK | O_DIRECTORY) = 0

[f] 'Tue Feb 19 14:24:56 2013' '/usr/sbin/chmac' <6914,5891,0,0,0> [s] parsec_chmac("/ald_export_home/petrovich/testdir/testfile2",{1,0x0},0) = 0

«. . . » . «Astra Linux Special Edition» . ping.

```
[p] 'Fri Feb 22 12:57:29 2013' '/bin/bash' <6798,6795,2500,2500,0> [s] exec("/bin/ping") = 0

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,0> [s] open("/etc/ld.so.cache",O_RDONLY) = 3

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,0> [s] open("/lib/libresolv.so.2",O_RDONLY) = 3

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,0> [s] open("/lib/libc.so.6",O_RDONLY) = 3

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,0> [s] setuid(2500) = 0

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] open("/etc/resolv.conf",O_RDONLY) = 4

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] open("/etc/resolv.conf",O_RDONLY) = 4

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] connect(SOCK_STREAM,{AF_UNIX,...},
{AF_UNIX,/var/run/nscd/socket}) = 0

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] connect(SOCK_STREAM,{AF_UNIX,...},
{AF_UNIX,/var/run/nscd/socket}) = 0

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] open("/etc/nsswitch.conf",O_RDONLY) =
4
```

```
[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] open("/etc/ld.so.cache",O_RDONLY) = 4

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] open("/lib/libnss_files.so.2",
O_RDONLY) = 4</

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] open("/etc/host.conf",O_RDONLY) = 4

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] open("/etc/hosts",O_RDONLY) = 4

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] open("/etc/ld.so.cache",O_RDONLY) = 4

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] open("/lib/libnss_dns.so.2",O_RDONLY)
= 4

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] connect(SOCK_DGRAM,{AF_INET,
10.0.0.106:41209},{AF_INET,10.0.0.1:53}) = 0

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] sendmsg(SOCK_DGRAM,{AF_INET,
10.0.0.106:41209},{AF_INET,10.0.0.1:53}) = 29

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] recvmsg(SOCK_DGRAM,{AF_INET,
10.0.0.106:41209},{AF_INET,10.0.0.1:53}) = 78

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] connect(SOCK_DGRAM,{AF_INET,
10.0.0.106:48650},{AF_INET,10.0.0.1:1025}) = 0

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] sendmsg(SOCK_RAW,{AF_INET,0.0.0.0:1},
{AF_INET,10.0.0.1:0}) = 64

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] recvmsg(SOCK_RAW,{AF_INET,0.0.0.0:1},
{AF_INET,10.0.0.1:0}) = 84

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] open("/etc/hosts",O_RDONLY) = 4

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] connect(SOCK_DGRAM,{AF_INET,
10.0.0.106:44260},{AF_INET,10.0.0.1:53}) = 0

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] sendmsg(SOCK_DGRAM,{AF_INET,
10.0.0.106:44260},{AF_INET,10.0.0.1:53}) = 39

[p] 'Fri Feb 22 12:57:29 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] recvmsg(SOCK_DGRAM,{AF_INET,
10.0.0.106:44260},{AF_INET,10.0.0.1:53}) = 96

[p] 'Fri Feb 22 12:57:30 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] sendmsg(SOCK_RAW,{AF_INET,0.0.0.0:1},
{AF_INET,10.0.0.1:0}) = 64

[p] 'Fri Feb 22 12:57:30 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] recvmsg(SOCK_RAW,{AF_INET,0.0.0.0:1},
{AF_INET,10.0.0.1:0}) = 84

[p] 'Fri Feb 22 12:57:30 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] open("/etc/hosts",O_RDONLY) = 4

[p] 'Fri Feb 22 12:57:30 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] connect(SOCK_DGRAM,{AF_INET,
10.0.0.106:53774},{AF_INET,10.0.0.1:53}) = 0

[p] 'Fri Feb 22 12:57:30 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] sendmsg(SOCK_DGRAM,{AF_INET,
10.0.0.106:53774},{AF_INET,10.0.0.1:53}) = 39

[p] 'Fri Feb 22 12:57:30 2013' '/bin/ping' <6798,6795,2500,2500,2500> [s] recvmsg(SOCK_DGRAM,{AF_INET,
10.0.0.106:53774},{AF_INET,10.0.0.1:53}) = 96
```

, IP- . 10 « «Astra Linux Special Edition». . 1».

1.2, 0, . , `/etc/pam.d/common-session` :

```
session optional pam_ald.so populate_krb5cc
```

, . .