FreeIPA

-
-
  - Astra Linux Special Edition
-
  -
  - pam- Astra Linux
  - pam- Astra Linux Special Edition
  -
  -
-
  - 524
  - mount error(126): Required key not available
-
  -

:

- Astra Linux Special Edition .10015-01 .10015-10 (1.7)
- Astra Linux Special Edition .10015-37 (7.7)
- Astra Linux Special Edition .10152-02 (4.7)
- Astra Linux Special Edition .10015-01 (1.6)
- Astra Linux Special Edition .10015-01 (1.5)
- Astra Linux Special Edition .10015-16 . 1 . 2
- Astra Linux Special Edition .10265-01 (8.1)

. CIFS (samba DFS)

Astra Linux Special Edition , Samba, :

1. Samba:

```
use socket MAC label = YES
```

(samba samba) . :

```
sudo net conf setparm global "use socket MAC label" "Yes"
```

2. Astra Linux Special Edition x.7 (SMB/CIFS)

Astra Linux Special Edition x.7 .

sec=krb5i,vers=1.0, server signing = required homes. :

a. ;
b. , samba [global] :

```
server max protocol = NT1
server signing = required
```

(samba samba) . :

```
sudo net conf setparm global "server max protocol" "NT1"
sudo net conf setparm global "server signing" "required"
```

/etc/samba/smb.conf, ;

3. , ( ), :

```
sudo smbcontrol all reload-config
```

, , , .

, . .

.

, .

- , FreeIPA Samba. . Samba + FreeIPA Samba Kerberos.
  Samba . . Samba + FreeIPA Samba Kerberos. FreeIPA + Samba, :
  - ipa0.ipadomain.ru;
  - admin;
  - - ipauser;
- - FreeIPA. . FreeIPA;

  .

, samba samba.

samba. :

1. ;
2. Astra Linux Special Edition. .

, samba. :

1. homes.txt:
   a. Astra Linux Common Edition, Astra Linux Special Edition , Astra Linux Special Edition :

```
cat << EOT > homes.txt
[homes]
   comment = Home Directories
   read only = No
   valid users = %S
EOT
```

   b. Astra Linux Special Edition :
      i. (, nomac). home "" , home :

```
cat << EOT > nomac.txt
[nomac]
    comment = NOMAC Home Dirs
    read only = No
    valid users = %U
    browseable = No
    create mask = 0600
    directory mask = 0700
    follow symlinks = yes
    path = /home/%U
EOT
```

ii. (path) home (home) /home/.pdp/<_>:

```
cat << EOT > homes.txt
[homes]
   comment = Home Directories
   read only = No
   valid users = %S
   browseable = No
   create mask = 0600
   directory mask = 0700
   follow symlinks = yes
   path = /home/.pdp/%U
EOT
```

2. samba homes.txt nomac.txt:

```
sudo net conf import homes.txt homes
sudo net conf import nomac.txt nomac
```

, , homes:

```
sudo net conf addshare "homes" "/home/%U" "writeable=y" "guest_ok=N" "Home
Directories"
sudo net conf setparm "homes" "browseable" "No"
sudo net conf setparm "homes" "valid users" "%U"
 ..
```

:

1. follow symlinks = yes :

```
sudo net conf setparm global "allow insecure wide links" yes
```

. man samba.conf;

2. sec=krb5i vers=1.0 (, x.7) [global] server signing=required:

```
sudo net conf setparm global "server signing" required
```

Astra Linux Special Edition

homes :

- — /home/<_> (homes,);
- :
  - - /home/.pdp/<_> (path = /home/.pdp/%U);
  - - /home/.pdp/<_>/<_> (path = /home/.pdp/%U);

, , , , , ("") . ipauser:

```
sudo mkdir -p /home/.pdp/ipauser/l0i0c0x0t0x0
sudo chown ipauser:ipauser /home/.pdp/ipauser
sudo pdpl-file 3:0:-1:CCNR /home/.pdp/ipauser
```

, 3, (-1).

FreeIPA. . FreeIPA Astra Linux.

, , :

1. pam_mount (Astra Linux Common Edition,);
2. (Astra Linux Special Edition,).

, .

pam_mount

, :

```
sudo apt install cifs-utils libpam-mount
```

pam_mount

pam_mount (/etc/security/pam_mount.conf.xml) (.). (,):

1. Astra Linux Common Edition, Astra Linux Special Edition , Astra Linux Special Edition (/home/<_>):

homes -

```
<volume
  fstype="cifs"
  server="ipa0.ipadomain.ru"
  path="%(USER)"
  mountpoint="/home/%(USER)"
  options="user=%(USER),cruid=%(USER),nosharesock,sec=krb5i"
/>
```

2. Astra Linux Special Edition :

   a. /home/.<_>:

```
<volume
  fstype="cifs"
  server="ipa0.ipadomain0.ru"
  path="nomac"
  mountpoint="/home/%(USER)"
  options="user=%(USER),cruid=%(USER),uid=%(USERUID),gid=%(USERGID),nosharesock,sec=krb5i"
/>
```

nomac;

   b. /home/.pdp/<_>:

Astra Linux Special Edition - pdp_homes

```
<volume
  fstype="cifs"
  server="ipa0.ipadomain.ru"
  path="%(USER)"
  mountpoint="/home/.pdp/%(USER)"
  options="user=%(USER),cruid=%(USER),uid=%(USERUID),gid=%(USERGID),nosharesock,sec=krb5i"
/>
```

, , /home/.pdp/<_> :

   i. - /home/.pdp/<_> (path = /home/.pdp/%U);
   ii. - /home/.pdp/<_>/<_> (path = /home/.pdp/%U);

, :

```
<mntoptions allow="nosuid,nodev,loop,encryption,fsck,nonempty,allow_root,allow_other,uid,gid,nosharesock,
vers" />
```

, (wait,) hup="yes", term="yes" kill="yes" "" :

```
<logout wait="0" hup="no" term="no" kill="yes" />
```

pam- Astra Linux

Astra Linux Common Edition Astra Linux Special Edition PAM-. session pam_mount /etc/pam.d/common-session pam_mount :

```
session [success=1 default=ignore] pam_localuser.so
session optional pam_mount.so
```

pam- Astra Linux Special Edition

() pam_mount /etc/pam.d/common-session:

```
sudo sed -i "s/\(session[[:space:]]\+optional[[:space:]]\+pam_mount.
so\)/#\1/" /etc/pam.d/common-session
```

/etc/pam.d/login /etc/pam.d/fly-dm session required pam_parsec_mac : , (pam_localuser.so), (pam_mount.so):

```
...
session required pam_parsec_mac.so ...
session [success=1 default=ignore] pam_localuser.so
session optional pam_mount.so
...
```

:

```
TARGET                                SOURCE.../home/ipauser01                    //ipa0.ipadomain.ru/nomac
/home/.pdp/ipauser01                //ipa0.ipadomain.ru/ipauser01
```

:

```
TARGET                                SOURCE
/home/ipauser01                     //ipa0.ipadomain0.ru/nomac
/home/.pdp/ipauser01                //ipa0.ipadomain0.ru/ipauser01
 /home/.pdp/ipauser01/l0i0c0x0t0x0 //ipa0.ipadomain0.ru/nomac
/var/private/tmp/l0i0c0x0t0x0       /dev/vda1[/tmp]
/tmp                                /dev/vda1[/var/private/tmp/l1i0c0x0t0x0]
/var/private/vartmp/l0i0c0x0t0x0    /dev/vda1[/var/tmp]
/var/tmp                            /dev/vda1[/var/private/vartmp/l1i0c0x0t0x0]
```

cifs-utils:

```
sudo apt install cifs-utils
```

pam_exec.

homes /home/.pdp/%U:

```
path = /home/.pdp/%U
```

:

Astra Linux Special Edition , , , :

/etc/pam.d/pdp_home.sh

```
#!/bin/bash
pdp_home=/home/.pdp/$PAM_USER
label="l`pdp-id -l`i`pdp-id -i`c`pdp-id -c`t0x0"
echo "Begin mounting PDP_HOME for user \"$PAM_USER\" with label \"$label\""
mount //ipa0.ipadomain0.ru/$PAM_USER $pdp_home -o user=$PAM_USER,sec=krb5i,rw,setuids,perm,soft,
iocharset=utf8,nosharesock,cruid=$PAM_USER
mount --bind $pdp_home/$label /home/$PAM_USER
```

pam_mount pam_mount, pam- session pam_parsec_mac /etc/pam.d/login /etc/pam.d/fly-dm. /etc/pam.d/pdp_home.sh, pam- :

/etc/pam.d/pdp_home.sh

```
session required pam_parsec_mac.so
session [success=1 default=ignore] pam_localuser.so
session optional pam_exec.so debug log=/dev/tty /etc/pam.d/pdp_home.sh
```

debug - , log=/dev/tty - ( ).

524

sec=krb5i vers=1.0 samba server signing = required.
- .

mount error(126): Required key not available

Kerberos. cifs.upcall :

```
sudo grep cifs.upcall /var/log/syslog
```

cruid=UID (ID).

log level, :

```
log level = 5
```

/var/log/samba/ (. log file).

:

```
sudo -s
modprobe cifs
echo 'module cifs +p' > /sys/kernel/debug/dynamic_debug/control
echo 'file fs/cifs/* +p' > /sys/kernel/debug/dynamic_debug/control
echo 7 > /proc/fs/cifs/cifsFYI
exit
```

, :

```
sudo dmesg
```

:

```
sudo -s
echo 0 > /proc/fs/cifs/cifsFYI
exit
```