CIFS (samba DFS)

:

- Astra Linux Special Edition .10015-01 (1.7)
- Astra Linux Special Edition .10015-10 ( )
- Astra Linux Special Edition .10015-17
- Astra Linux Special Edition .10015-37 (7.7)
- Astra Linux Special Edition .10015-03 (7.6)
- Astra Linux Special Edition .10152-02 (4.7)
- Astra Linux Special Edition .10015-01 (1.6)
- Astra Linux Special Edition .10015-16 . 1
- Astra Linux Special Edition .10015-16 . 2
- Astra Linux Special Edition .10265-01 (8.1)
- Astra Linux Common Edition 2.12 ( )

. : FreeIPA

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
```

:

- - Samba. FreeIPA , .. samba, FreeIPA (--setup-adtrust). FreeIPA samba Samba + FreeIPA Samba Kerberos. **ipa0.ipadomain.ru**.
- -. , FreeIPA.

samba

samba Samba

, , :

:

```
sudo mkdir /share1
```

, Astra Linux Special Edition, :

```
sudo mkdir -p /share1/{zero,dsp,secret,topsecret}
```

, :

```
sudo chmod 777 /share1 -R
```

"4. " " . 1 .10015-01 97 01-1"():

```
sudo pdpl-file 3:0:-1:ccnr /share1/
sudo pdpl-file 1:0:0 /share1/dsp
sudo pdpl-file 2:0:0 /share1/secret
sudo pdpl-file 3:0:0 /share1/topsecret
```

samba

/etc/samba/smb.conf :

/etc/samba/smb.conf

```
[global]
#
workgroup = WORKGROUP
#    netbios
disable netbios = no
# ,    ,
map to guest = Bad User

[share1]
comment = For all doc's
#
guest ok = yes
path = /share1
read only = no
available = yes
browseable = yes
case sensitive = yes
ea support = yes
fstype = Samba
smb encrypt = auto
```

, samba- "" **fly-fm** **NetBIOS**
/etc/samba/smb.conf "disable netbios = no" ( ).

```
disable netbios = no
```

```
testparm
```

testparm , Samba:

```
sudo systemctl restart smbd
```

,

```
smbtree
```

.

[homes] -

[homes] - .
, .

, , :

- [global]

  passdb backend = smbpasswd

- samba

  ```
  sudo systemctl restart smbd
  ```

- samba:

  ```
  smbpasswd -a username
  ```

[homes] /etc/samba/smb.conf :

```
[homes]
comment = Home Directories
valid users = %S
#  [homes]  (read only = yes).
#  read only = no
read only = No
create mask = 0700
directory mask = 0700
browseable = no
guest ok = no
```

, (, smbclient username):

```
smbclient //ipa0.ipadomain.ru/username
```

, :

```
smbclient //ipa0.ipadomain.ru/username -U username
```

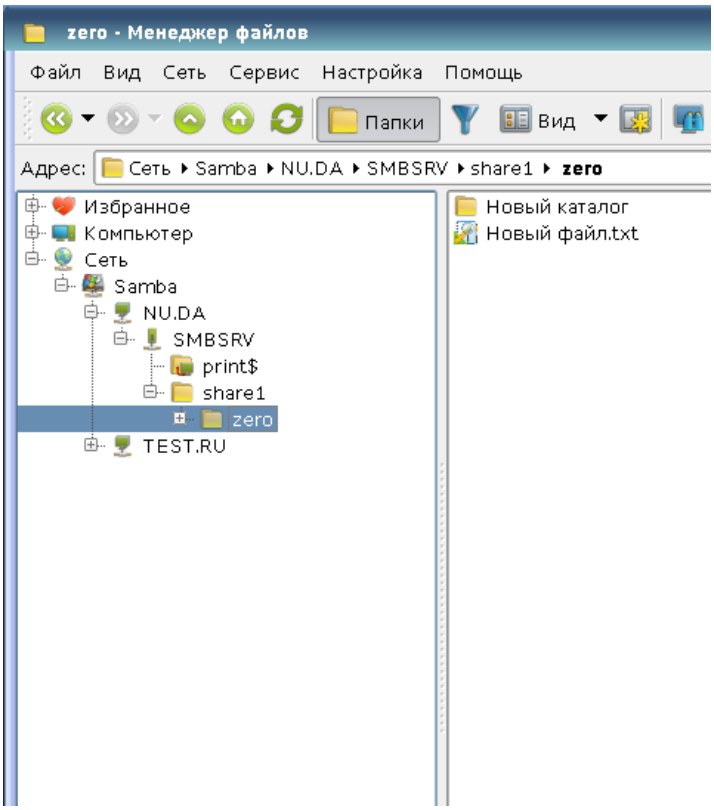
samba , [homes].
, , (, /etc/passwd).
, samba .
/etc/passwd, .

[homes] path, , /home, .. /home/username, , , /samba/users/username:

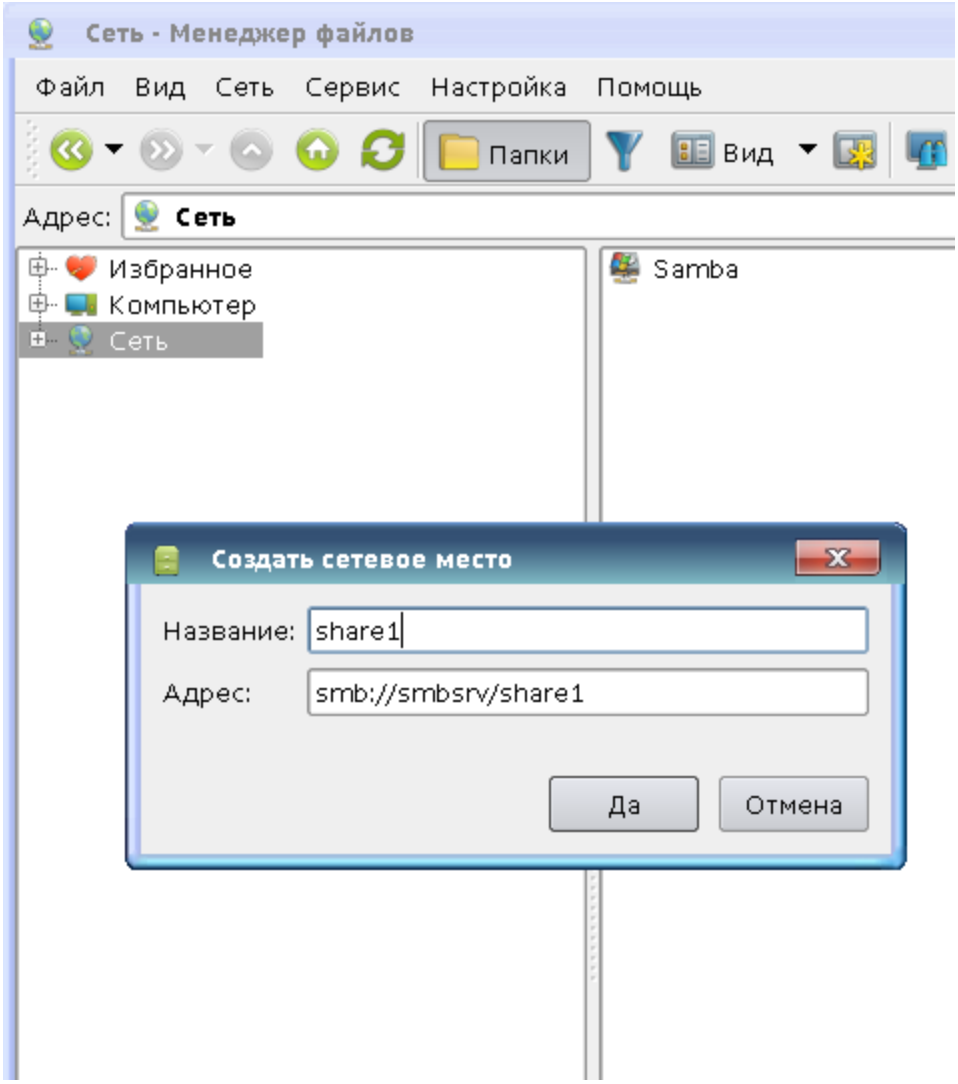
```
[homes]
comment = Home Directories
valid users = %S
path = /samba/users/%S
read only = No
create mask = 0700
directory mask = 0700
browseable = no
guest ok = no
```

samba

(**fly-fm**) "", **Samba** **NetBIOS** :



NetBIOS , , "" "":



fly-fm .

CIFS/Samba

- cifs-utils:

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

`mount` , :

```
sudo mount.cifs /// /_ [-o ]
sudo mount -t cifs /// /_ [-o ]
```

, , , , .. /media/*share1* , :

```
sudo mkdir /media/share1
sudo chmod 777 /media/share1
sudo mount -t cifs //fileserver1.org.net/share1 /media/share1 -o user=
```

/etc/fstab sudo.
/etc/fstab , :

//fileserver1.org.net/share1 /media/share1 cifs user,rw,noauto,iocharset=utf8,soft 0 0

/, user .
mount :

```
mount /media/share1
```

`man mount mount.cifs`. */etc/fstab* `man` *fstab*.

/etc/fstab :

//fileserver1.org.net/share1 /media/share1 cifs user,rw,noauto,iocharset=utf8,nosharesock,vers=1.0,soft 0 0

Kerberos sec=krb5i sec=krb5. Kerberos .

Kerberos Kerberos, FreeIPA Astra Linux.
. FreeIPA Kerberos.

pam_mount

PAM- **pam_mount**, **libpam-mount**, - cifs-utils libpam_mount:

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

libpam-mount PAM-.
(/etc/pam.d/,).
, pam_mount PAM- .
, Kerberos (. FreeIPA Astra Linux).

pam_mount */etc/security/pam_mount.conf.xml*.

libpam_mount pam_mount **pam-** (*common-auth*, *common-session*) */etc/pam.d*.

pam_mount `man` **pam_mount** **pam_mount.conf**.

pam-mount , :

/etc/security/pam_mount.conf.xml

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE pam_mount SYSTEM "pam_mount.conf.xml.dtd">
<!--
    See pam_mount.conf(5) for a description.
-->
<pam_mount>
    <!-- debug should come before everything else,
         since this file is still processed in a single pass
         from top-to-bottom -->
    <debug enable="1" />
    <!-- Volume definitions -->
    <cifsmount>mount.cifs //%(SERVER)/%(VOLUME) %(MNTPT) -o %(OPTIONS) </cifsmount>
    <!-- pam_mount parameters: General tunables -->
    <!--  ,    -->
    <volume
        fstype="cifs"
        server="ipa0.ipadomain.ru"
        path="share1"
        mountpoint="/media/%(USER)"
```

```
        options="user=%(USER),cruid=%(USER),sec=krb5i,file_mode=0770,dir_mode=0770"
    />

    <!--
    <luserconf name=".pam_mount.conf.xml" />
    -->

    <!-- Note that commenting out mntoptions will give you the defaults.
         You will need to explicitly initialize it with the empty string
         to reset the defaults to nothing. -->
    <mntoptions allow="nosuid,nodev,loop,encryption,fsck,nonempty,allow_root,allow_other" />
    <!--
    <mntoptions deny="suid,dev" />
    <mntoptions allow="*" />
    <mntoptions deny="*" />
    -->
    <mntoptions require="nosuid,nodev" />

    <logout wait="50000" hup="1" term="1" kill="1" />
    <!-- <logout wait="0" hup="no" term="no" kill="no" /> -->
    <!-- pam_mount parameters: Volume-related -->
    <mkmountpoint enable="1" remove="true" />
</pam_mount>
```

/media/username. , . mountpoint="/home/%(USER)/share1" /share1/ . Astra Linux Special Edition , , PAM-, , pam_mount . :

1. pam_mount /etc/pam.d/common-session;
2. /etc/pam.d/login /etc/pam.d/fly-dm Astra Linux:

FreeIPA ( ):

session required pam_parsec_mac.so
session optional pam_mount.so

ALD ( ):

session required pam_parsec_mac.so
session required pam_ald.so
session optional pam_mount.so

(, samba home):

```
...
<volume
        fstype="cifs"
        server="ipa0.ipadomain.ru"
        path="%(USER)"
        mountpoint="/home/%(USER)"
        options="user=%(USER),cruid=%(USER),sec=krb5i,file_mode=0770,dir_mode=0770"
/>
...
```

Kerberos sec=krb5i (,) sec=krb5. **Kerberos** .

cruid=%(USER), .

mountpoint , : /media/ald_share. :

path="share" mountpoint="/media/ald_share" options="user=%(USER),rw,setuids,perm,soft,sec=krb5i,cruid=%(USERUID),file_mode=0770, dir_mode=0770,iocharset=utf8,vers=1.0" />

logout . , .

mkmountpoint .

cifsmount , .

volume .

pam_mount

[homes], /home/<_> . pam_mount:

/etc/security/pam_mount.conf.xml

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE pam_mount SYSTEM "pam_mount.conf.xml.dtd">
<!--
        See pam_mount.conf(5) for a description.
-->

<pam_mount>
    <!-- debug should come before everything else,
         since this file is still processed in a single pass
         from top-to-bottom -->
    <debug enable="1" />

    <!-- Volume definitions -->
    <!--    homes    -->
    <cifsmount>mount.cifs //%(SERVER)/%(USER) %(MNTPT) -o %(OPTIONS) </cifsmount>
    <!-- pam_mount parameters: General tunables -->
    <!--  ,    -->
    <volume
        fstype="cifs"
        server="ipa0.ipadomain.ru"
        path="%(USER)"
        mountpoint="/home/%(USER)"
        options="rw,user=%(USER),gid=%(USER),uid=%(USER),cruid=%(USER),sec=krb5i,file_mode=0770,
dir_mode=0770"
    />
    <!--
        <luserconf name=".pam_mount.conf.xml" />
    -->

    <!-- Note that commenting out mntoptions will give you the defaults.
         You will need to explicitly initialize it with the empty string
         to reset the defaults to nothing. -->
    <mntoptions allow="nosuid,nodev,loop,encryption,fsck,nonempty,allow_root,allow_other" />
    <!--
    <mntoptions deny="suid,dev" />
    <mntoptions allow="*" />
    <mntoptions deny="*" />
    -->
    <mntoptions require="nosuid,nodev" />

    <logout wait="50000" hup="1" term="1" kill="1" />
        <!-- <logout wait="0" hup="no" term="no" kill="no" /> -->
    <!-- pam_mount parameters: Volume-related -->
    <mkmountpoint enable="1" remove="true" />
</pam_mount>
```

SAMBA AD winbind - user=%(DOMAIN_USER).

luserconf

pam_mount . , luserconf */etc/security/pam_mount.conf.xml* pam_mount. :

```
luserconf name="<___>"
```

:

```
<luserconf name=".pam_mount.conf.xml" />
```

. . , , . . , . , , , , luserconf.

:

- mntoptions allow - , :

  ```
  <mntoptions allow="user,cruid,vers,sec,nosuid,nodev,loop,encryption,fsck,nonempty,allow_root,
  allow_other" />
  ```

  nosuid nodev, , , ;
- mntoptions deny - . ;
- mntoptions require - . nosuid nodev. , , ;

DFS

Distributed File System (DFS) Microsoft Windows . DFS, samba, cifs.

DFS keyutils:

```
sudo apt install keyutils
```

DFS (, ,), linux_5.4.0-110.astra35+ci1 linux-5.10_5.10.0-1057.astra6+ci7.

DFS , :

:

```
mount -t cifs //server1.active_directory.test/dfs1 ~/mnt -o cruid=user1,
sec=krb5
```

:

```
mount -t cifs //active_directory.test/dfs1 ~/mnt -o cruid=user1,sec=krb5
```

DFS Kerberos :

1. . — . : SETSPN:

   ```
   SETSPN -s cifs/<_> <_>
   ```

   :

   ```
   SETSPN -s cifs/ad12.loc w12
   ```

2. "-t" /etc/request-key.d/cifs.spnego.conf:

   , "-t" , DNS- (DNS-), .

   ```
   create cifs.spnego * * /usr/sbin/cifs.upcall -t %k
   ```

, DFS , samba, CIFS, .

pam_mount, :

```
reenter password for pam_mount
```

.

> pam_mount, , .

/etc/pam.d/common-session :

```
session optional pam_mount.so
```

:

```
session optional pam_mount.so disable_interactive
```