

Samba + FreeIPA Samba Kerberos

-
- samba FreeIPA
- samba FreeIPA
- FreeIPA - samba
- /
- samba
-
-
-



:

- Astra Linux Special Edition .10015-01 (1.7) [2022-0819SE17 \(1.7.2\)](#)
- Astra Linux Special Edition .10015-10 (1.7) [2022-0819SE17 \(1.7.2\)](#)
- Astra Linux Special Edition .10152-02 (4.7) 4.7.2
- Astra Linux Special Edition .10015-01 (1.6) [20220829SE16 \(11\)](#)
- Astra Linux Common Edition 2.12.45

, FreeIPA (). samba winbind.

samba FreeIPA

samba FreeIPA. :

- FreeIPA astra-freeipa-server — -s;
- astra-freeipa-replica — --setup-adtrust .

Samba Windows AD, Windows AD .

samba FreeIPA

() FreeIPA samba, :

1. Kerberos :

```
sudo kinit admin
```

2. :

```
sudo ipa-adtrust-install --add-sids --add-agents
```

FreeIPA - samba

samba:

- samba ROLE_DOMAIN_PDC;
- samba FreeIPA;
- CIFS.



"ipa service-add ...", -, : .



ipa-adtrust-install samba .
samba _.
-.

samba winbind ipactl, , smb winbind:

```
sudo ipactl status
```

```
...
smb Service: RUNNING
winbind Service: RUNNING
...
```

```
samba /etc/samba/smb.conf "registry", :
```

 ### Added by IPA Installer ###
[global]
debug pid = yes
config backend = registry

 "config backend = registry", registry, /etc/samba/smb.conf .
,"config backend = registry" "include = registry", /etc/samba/smb.conf.

```
testparm, :
```

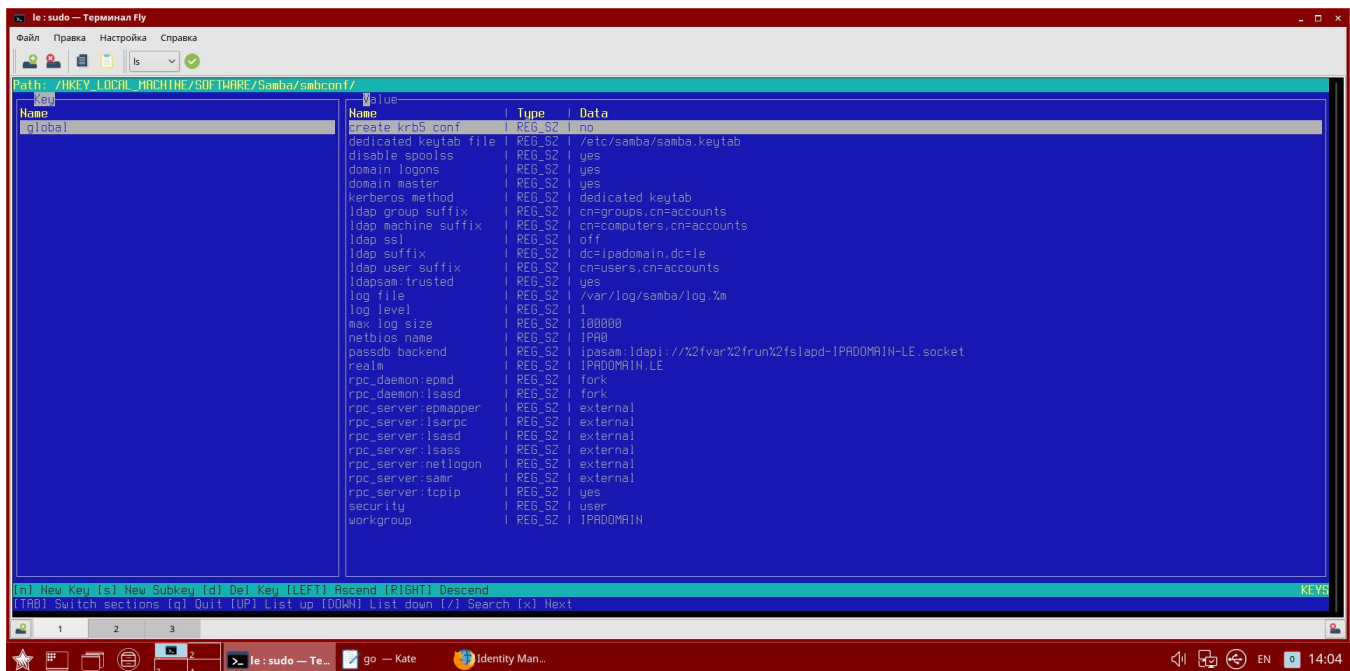
```
sudo testparm
```

 "registry" (sudo testparm), .

```
"registry" samba-regedit ( samba):
```

```
sudo samba-regedit
```

```
samba /HKEY_LOCAL_MACHINE/SOFTWARE/Samba/smbconf:
```



```
samba ( , homes) . REG_SZ.
```

```
registry samba net, homes share:
```

```
1. homes.txt homes:
```

 [homes]
browseable = no
comment = Home Directories

```
create mask = 0600
directory mask = 0700
valid users = %S
# [homes] (read only = yes).
# read only = no
read only = No
guest ok = no
```

2. share.txt share:

 [share]
comment = anonymous share
create mask = 0666
directory mask = 0777
guest ok = yes
guest only = yes
path = /srv/share
read only = no

3. samba:

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

,, 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" "%S"
```

..

 registry ,, , samba .

admin (.. FreeIPA, " "):

 sudo mkhomedir_helper admin

/

(- . homes) Kerberos:

```
kinit admin
smbclient -k //ipa0.ipadomain.ru/admin
```

Kerberos Kerberos (cruid, user, sec):

```
sudo mount -t cifs //ipa0.ipadomain.ru/share /media/share -o cruid=admin,
user=admin,sec=krb5i
```

 sec=krb5i :

```
server signing = required
```

():

```
sudo mount -t cifs //ipa0.ipadomain.ru/share /media/share -o cruid=admin,
user=admin,sec=krb5
```

samba

samba . samba Kerberos , FreeIPA.

1. :

a. samba, , :

```
sudo kinit admin
sudo ipa-adtrust-install --add-sids --add-agents
```

b. (SID) (SID for domain):

```
sudo net getdomainsid
```

:

```
SID for local machine IPA0 is: S-1-5-21-2933183829-3187441131-1463459236
SID for domain IPADOMAIN is: S-1-5-21-2933183829-3187441131-1463459236
```

SID for domain samba, [samba](#) ;

c. :

```
sudo ipa idrange-find --raw
```

:

```
-----
1 range matched
-----
cn: IPADOMAIN.RU_id_range
ipabaseid: 72000
ipaidrangesize: 1000000
ipabaserid: 1000
ipasecondarybaserid: 100000000
iparangetype: ipa-local
-----
1
-----
```

[ipabaseid](#) [ipaidrangesize](#), [ipabaseid](#) () , :

```
ipabaseid + ipaidrangesize -1
```

2. :

- IP- ([Astra Linux](#));
- .. [FreeIPA](#);
- :



libwbclient-sssd:

- Astra Linux Special Edition x.7 ;
- Astra Linux Special Edition .10015-01 (1.6) .

`sudo apt install libwbclient-sssd samba winbind freeipa-admintools`

`freeipa-admintools , , , samba ;`

3. , (freeipa-admintools) :

a. Kerberos :

`kinit admin`

b. (: cifs - samba, samba.ipadomain.ru - ,):

`ipa service-add cifs/samba.ipadomain.ru`

c. (,):

```
ipa permission-add "CIFS server can read user passwords" --attrs={ipaNTHash,ipaNTSecurityIdentifier} --type=user --right={read,search,compare} --bindtype=permission
ipa privilege-add "CIFS server privilege"
ipa privilege-add-permission "CIFS server privilege" --permission="CIFS server can read user passwords"
ipa role-add "CIFS server"
ipa role-add-privilege "CIFS server" --privilege="CIFS server privilege"
```

d. :

`ipa role-add-member "CIFS server" --services=cifs/samba.ipadomain.ru`

4. :

a. (/srv/share/) "._" (nobody nogroup):

```
sudo mkdir -p /srv/share
sudo chown nobody:nogroup /srv/share
```

b. ():

```
sudo kinit admin
sudo ipa-getkeytab -s ipa0.ipadomain.ru -p cifs/samba.ipadomain.ru -k /etc/samba/samba.keytab
```

```
:
- ipa0.ipadomain.ru — , ;
- cifs/samba.ipadomain.ru — , ;
- /etc/samba/samba.keytab — , ;
```

c. samba, /etc/samba/smb.conf :



```
[global]
dedicated keytab file = /etc/samba/samba.keytab
kerberos method = dedicated keytab
log file = /var/log/samba/log.%m
realm = IPADOMAIN.RU
security = ads
workgroup = IPADOMAIN
idmap config IPADOMAIN : range = < > < >
idmap config IPADOMAIN : backend = sss
idmap config * : range = 0 - 0
```

```
[homes]
browsable = no
writable = yes

[shared]
path = /srv/share
writable = yes
browseable = yes
```

```
:
- realm = IPADOMAIN.RU — Kerberos, ;
- workgroup = IPADOMAIN — , () Kerberos;
- idmap config IPADOMAIN : range FreeIPA;
- [homes] [shared] ( [homes] ,. Samba);
```

d. :

```
sudo net setdomainsid <SID>
```

```
:
- <SID> — ;
```

e. samba:

```
sudo systemctl restart smbd winbind
```

.

, samba :

1. :

```
kinit admin
```

2. , ., shareaccess:

```
ipa group-add shareaccess
```

3. , ., ipauser01 ipauser02:

```
ipa group-add-member shareaccess --users=ipauser01 --users=ipauser02
```

4. valid users (. "@",), share shareaccess admin. samba samba, :

```
sudo net conf setparm "share" "valid users" "@shareaccess,admin"
```

samba , (smbd).

samba () , , :

1. :

```
kinit <__>
```

2. samba Kerberos:

```
smbclient -kL <_>
```

3. Kerberos samba . :

- a. Kerberos :

```
kdestroy -A
```

- b. :

```
smbclient -kL <_>
```

- NT_STATUS_BAD_NETWORK_NAME , (homes -);
- NT_STATUS_INVALID_PARAMETER Kerberos , Kerberos (- sudo, sudo);
- "mkdir failed on directory /var/run/samba/msg.lock: " samba , :

```
sudo mkdir /run/samba/msg.lock
```

```
, , /usr/lib/tmpfiles.d/samba.conf "d /run/samba 0755 root root -" "d /run/samba/msg.lock 0755 root root -";
```

```
sudo sed -i "s~^s*d\s*/run/samba\s*0755\s*root\s*root\s*~d /run/samba/msg.lock 0755 root root ~" /usr/lib/tmpfiles.d/samba.conf
```

- "open_internal_pipe: Could not connect to dssetup pipe: NT_STATUS_RPC_INTERFACE_NOT_FOUND" winbind ;
- "Unable to initialize messaging context" samba ;