Файловый сервер SAMBA с доступом по группам FreeIPA и аутентификацией по Kerberos

Дата экспорта 27 августа 2020

v4

На момент настройки файлового сервера, компьютер (файловый сервер) должен являться клиентом домена FreeIPA.

Допустим у нас есть настроенный контроллер домена dc1.astra.loc .

Клиент домена, который нужно настроить в качестве файлового сервера fs.astra.loc .

И клиент домена для тестирования подключения сетевых папок client1.astra.loc .

Все команды выполняются из под учетной записи администратора домена и от "sudo" .

1 Подготовка контроллера домена FreeIPA

Устанавливаем необходимые пакеты на серверах:

```
sudo apt install freeipa-server-trust-ad libwbclient-sssd samba smbclient
```

На контроллере домена нужно добавить сервис cifs для работы Samba:

```
sudo ipa service-add cifs/fs.astra.loc
```

Добавляем права для Samba сервера:

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"

ipa role-add-member "CIFS server" --services=cifs/fs.astra.loc

```
admin@dc1:~$ ipa role-add "CIFS server"
----------------------------
Добавлена роль "CIFS server"
----------------------------
  Имя роли: CIFS server
admin@dc1:~$ ipa role-add-privilege "CIFS server" --privilege="CIFS server privilege"
  Имя роли: CIFS server
  Privileges: CIFS server privilege
----------------------------------
Количество добавленных привилегий 1
----------------------------------
admin@dc1:~$ ipa role-add-member "CIFS server" --services=cifs/fs.astra.loc
  Имя роли: CIFS server
  Privileges: CIFS server privilege
  Службы-участники: cifs/fs.astra.loc@ASTRA.LOC
----------------------------------
Количество добавленных участников 1
----------------------------------
```

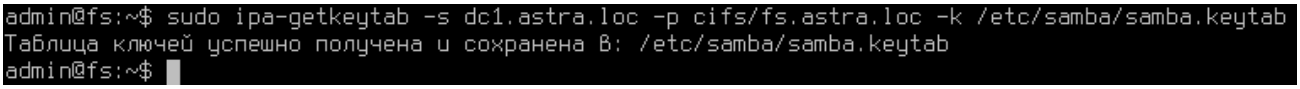
2 Настройка файлового сервера

Устанавливаем необходимые пакеты на серверах:

```
sudo apt install freeipa-server-trust-ad libwbclient-sssd samba smbclient
```

В консоль на файловом сервере делаем:

```
sudo ipa-getkeytab -s dc1.astra.loc -p cifs/fs.astra.loc -k /etc/samba/
samba.keytab
```



(Не обязательно) Делаем проверку, путем чтения атрибутов пользователя в домене. Перед использованием проверить дату истечения билета Kerberos (klist) и при необходимости сделать kinit admin.

```
ldapsearch -Y gssapi "(uid=ipauser1)"
```

Результат выполнения команды

ipauser1@fs:~$ ldapsearch -Y gssapi "(uid=ipauser1)"
SASL/GSSAPI authentication started
SASL username: ipauser1@ASTRA.LOC
SASL SSF: 56
SASL data security layer installed.
extended LDIF
#
LDAPv3
base <dc=astra,dc=loc> (default) with scope subtree
filter: (uid=ipauser1)
requesting: ALL
#

ipauser1, users, compat, astra.loc
dn: uid=ipauser1,cn=users,cn=compat,dc=astra,dc=loc
objectClass: posixAccount
objectClass: ipaOverrideTarget
objectClass: top
gecos: 11 11
cn: 11 11
uidNumber: 192001
gidNumber: 192001
loginShell: /bin/bash
homeDirectory: /home/ipauser1

ipaAnchorUUID::
OklQQTphc3RyYS5kb206NzRkMWRkNzItMmE1ZC0xMWVhLTliMGUtMDgwMDI3ND
IwN2Fl
uid: ipauser1

ipauser1, users, accounts, astra.loc
dn: uid=ipauser1,cn=users,cn=accounts,dc=astra,dc=loc
displayName: 11 11
uid: ipauser1
krbCanonicalName: ipauser1@ASTRA.LOC
objectClass: top
objectClass: person
objectClass: organizationalperson
objectClass: inetorgperson
objectClass: inetuser
objectClass: posixaccount
objectClass: krbprincipalaux
objectClass: krbticketpolicyaux
objectClass: ipaobject
objectClass: ipasshuser
objectClass: ipaSshGroupOfPubKeys
objectClass: mepOriginEntry
objectClass: ipantuserattrs
loginShell: /bin/bash
initials: 11
gecos: 11 11
sn: 11
homeDirectory: /home/ipauser1
mail: ipauser1@astra.loc
krbPrincipalName: ipauser1@ASTRA.LOC
givenName: 11
cn: 11 11
ipaUniqueID: 74d1dd72-2a5d-11ea-9b0e-0800274207ae
uidNumber: 192001
gidNumber: 192001
mepManagedEntry: cn=ipauser1,cn=groups,cn=accounts,dc=astra,dc=loc
memberOf: cn=admins,cn=groups,cn=accounts,dc=astra,dc=loc
memberOf: cn=Replication Administrators,cn=privileges,cn=pbac,dc=astra,dc=loc
memberOf: cn=Add Replication Agreements,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=Modify Replication Agreements,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=Read Replication Agreements,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=Remove Replication Agreements,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=Modify DNA Range,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=Read PassSync Managers Configuration,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=Modify PassSync Managers

Configuration,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=Read LDBM Database Configuration,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=Add Configuration Sub-Entries,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=Read DNA Range,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=Host Enrollment,cn=privileges,cn=pbac,dc=astra,dc=loc
memberOf: cn=System: Add krbPrincipalName to a Host,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=System: Enroll a Host,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=System: Manage Host Certificates,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=System: Manage Host Enrollment
Password,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=System: Manage Host Keytab,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=System: Manage Host Principals,cn=permissions,cn=pbac,dc=astra,dc=loc
memberOf: cn=ipausers,cn=groups,cn=accounts,dc=astra,dc=loc
ipaNTSecurityIdentifier: S-1-5-21-1258707283-2585043547-335861022-1001
krbLastPwdChange: 20191229175204Z
krbPasswordExpiration: 20200328175204Z
krbLoginFailedCount: 0
krbExtraData:: AALE5whea2FkbWluZEBBU1RSQS5ET00A
krbTicketFlags: 128
krbLastFailedAuth: 20200119095425Z

search result
search: 4
result: 0 Success

numResponses: 3
numEntries: 2

Создаем папку к которой откроем сетевой доступ:

```
admin@fs:/$ sudo mkdir /srv/shared
admin@fs:/$ sudo chown root:shareaccess /srv/shared
admin@fs:/$ sudo chmod 770 /srv/shared
admin@fs:/$ sudo ls -la /srv
итого 12
drwxr-xr-x  3 root root        4096 янв 20 16:36 .
drwxr-xr-x 27 root root        4096 янв 20 16:36 ..
drwxrwx---  2 root shareaccess 4096 янв 20 16:36 shared
```

Редактируем /etc/samba/smb.conf

```
[global]
        debug pid = Yes
        realm = ASTRA.LOC
        workgroup = ASTRA
        domain master = Yes
        domain logons = Yes

        ldap admin dn = cn=Directory Manager
        ldap group suffix = cn=groups,cn=accounts
        ldap machine suffix = cn=computers,cn=accounts
        ldap suffix = dc=astra,dc=loc
        ldap user suffix = cn=users,cn=accounts
        ldap ssl = no

        kerberos method = dedicated keytab
        dedicated keytab file = FILE:/etc/samba/samba.keytab
        disable spoolss = Yes
        create krb5 conf = No
        security = user

        log file = /var/log/samba/log.%m
        log level = 1
        max log size = 100000

        rpc_server:epmapper = external
        rpc_server:lsarpc = external
        rpc_server:lsass = external
        rpc_server:lsasd = external
        rpc_server:samr = external
        rpc_server:netlogon = external
        rpc_server:tcpip = yes
        rpc_daemon:epmd = fork
        rpc_daemon:lsasd = fork
        idmap config * : backend = tdb
        ldapsam:trusted = yes

[homes]
        comment = Home Directories
        valid users = %S, %D%w%S
        browseable = Yes
        read only = No
        create mask = 0600
        directory mask = 0700


[shared]
        comment = Test share on file server
        path = /home/shared
        browseable = yes
        valid users = @shareaccess
        write list = @shareaccess
```

```
        create mask = 0660
        directory mask = 0770
```

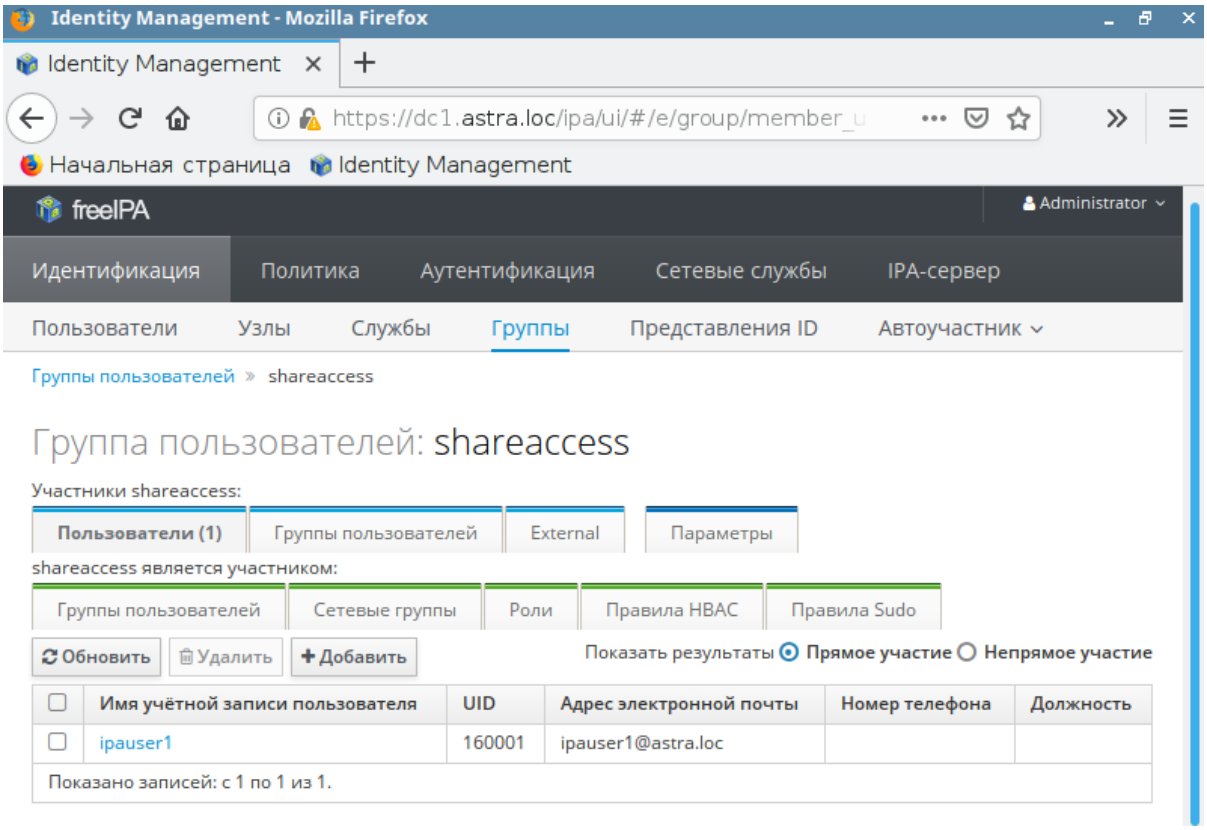
Делаем проверку smb.conf
Заставляем службу smbd перечитать измененный конфиг.
А также можно сделать перезапуск служб smb и winbind (Не обязательно. Это необходимо делать, если меняется имя сетевой папки.)

testparm

smbcontrol all reload-config (вместо "all" доступны опции "smbd", "nmbd" или "winbindd")

systemctl restart smbd winbind

Добавляем пользователя FreeIPA в группу "shareaccess" :



3 Доступ для нескольких групп

Добавляем в домен FreeIPA новую группу "group2" и включаем в нее нового пользователя "ipauser2" .

Выставляем дополнительные права на сетевую папку "shared", для группы "group2" .

setfacl -m g:group2:rwx /home/shared

getfacl /home/shared

```
admin@fs:~$ sudo setfacl -m g:group2:rwx /home/shared
admin@fs:~$ getfacl /home/shared
getfacl: Removing leading '/' from absolute path names
# file: home/shared
# owner: root
# group: shareaccess
user::r--
group::rwx
group:group2:rwx
mask::rwx
other::---

admin@fs:~$
```

Перед установкой прав на папку для новой группы (например group3), ее нужно сначала добавить в FreeIPA, иначе выходит ошибка :

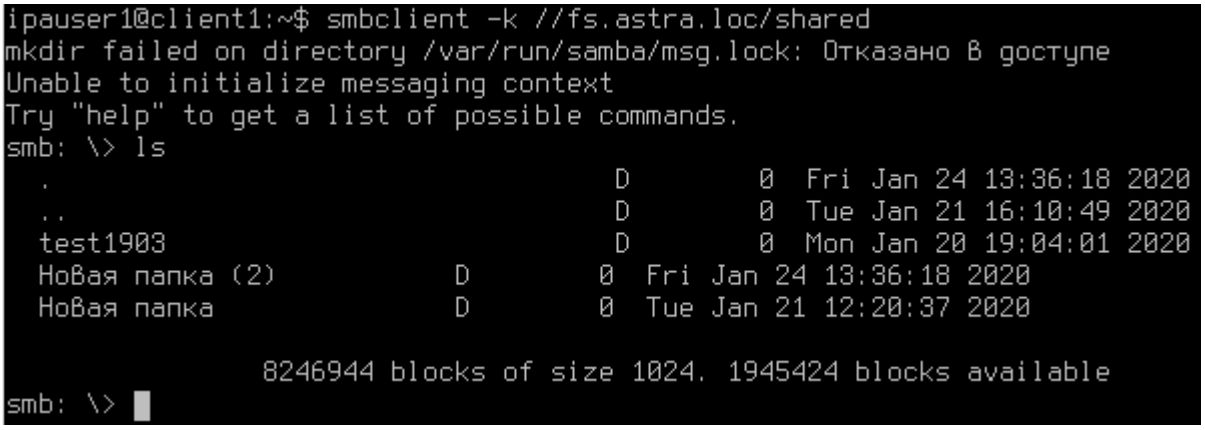
```
admin@fs:~$ sudo setfacl -m g:group3:rwx /home/shared
setfacl: Option -m: Недопустимый аргумент near character 3
```

4 Подключение сетевых папок на клиентском компьютере

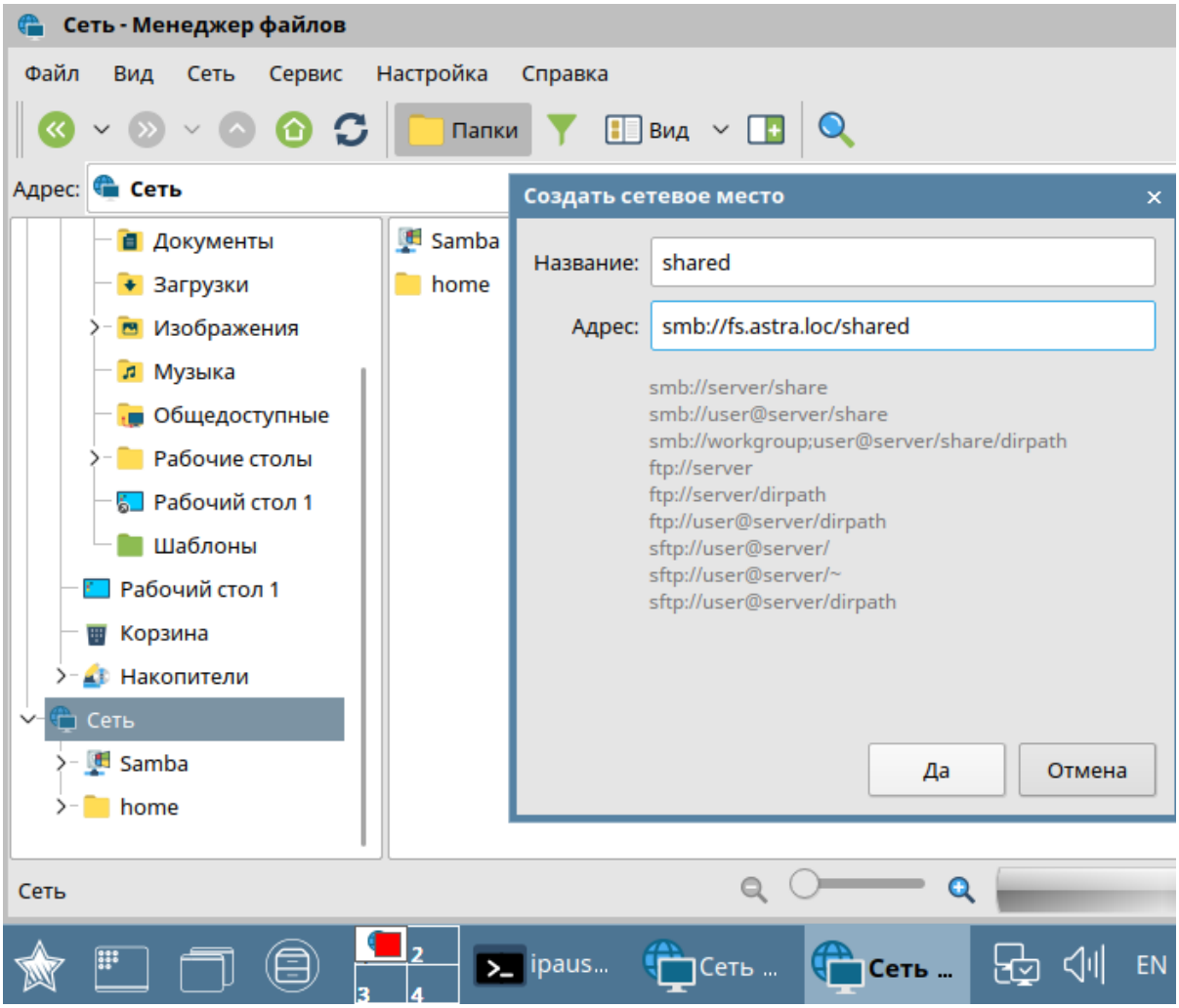
Для настройки подключения к сетевым папкам заходим на любой другой клиент домена под доменным пользователем "ipauser1" , который включен в группу "shareaccess".

Проверяем доступ к сетевой папке :

```
smbclient -k //fs.astra.loc/shared
```



Далее создаем подключение к сетевым папкам.
Запускаем "Файловый менеджер", переходим на вкладку "Сеть" и настраиваем сетевые папки "homes" и "shared".



В примере сетевая папка "shared" подключена с полным доступом для всех, кто включен в группу "shareaccess" .