# Samba + FreeIPA аутентификация пользователей Samba в Kerberos



Данная статья применима к:

- ОС ОН Орёл 2.12
- ОС СН Смоленск 1.6
- ОС СН Ленинград. 8.1

## Исходные данные

Предполагается, что у нас уже есть установленный сервер FreeIPA.
При стандартной установке FreeIPA на таком сервере уже установлены службы samba и winbind.

## Донастройка сервера FreeIPA

Если при установке сервера не была применена опция --setup-adtrust (установка компонент для работы с samba и Windows AD), то доустановить необходимые компоненты:

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

После этого:

- samba получит роль ROLE_DOMAIN_PDC;
- Сервис samba будет переведён под управление FreeIPA;
- Будет создана и зарегистрирована доменная служба CIFS.

Отдельно выполнять команду добавления службы "ipa service-add ...", как рекомендуется во многих Интернет-инструкциях, не нужно: служба добавится автоматически.

# Особенности работы связки FreeIPA - Samba

После установки ipa-adtrust-install чтение конфигурации samba на сервере будет доступно только суперпользователю.
Монитирование и авторизация через samba на сервере для простых пользователей работать **не будут**.
Монитировать разделяемые ресурсы следует только с компьютеров-клиентов.

Службы samba и winbind теперь будут управляться командой ipactl, в списке служб появится службы smb и winbind:

```
sudo ipactl status
```

```
Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmin Service: RUNNING
named Service: RUNNING
httpd Service: RUNNING
ipa-custodia Service: RUNNING
ntpd Service: RUNNING
smb Service: RUNNING
winbind Service: RUNNING
ipa-otpd Service: RUNNING
ipa-dnskeysyncd Service: RUNNING
ipa: INFO: The ipactl command was successful
```

В конфигурационном файле сервиса samba /etc/samba/smb.conf останется только отсылка в БД "registry", куда будут перенесены все конфигурационные параметры:

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

Опция "config backend = registry" указывает, что все конфигурационные параметры будут храниться в БД registry, а параметры, указанные в файле /etc/samba/smb.conf после этой опции будут игнорироваться.
Можно создать комбинированную конфигурацию, заменив "config backend = registry" на "include = registry", что позволит задавать параметры в файле /etc/samba/smb.conf.

Проверить конфигурацию можно стандартной командой testparm, однако теперь только от имени суперпользователя:

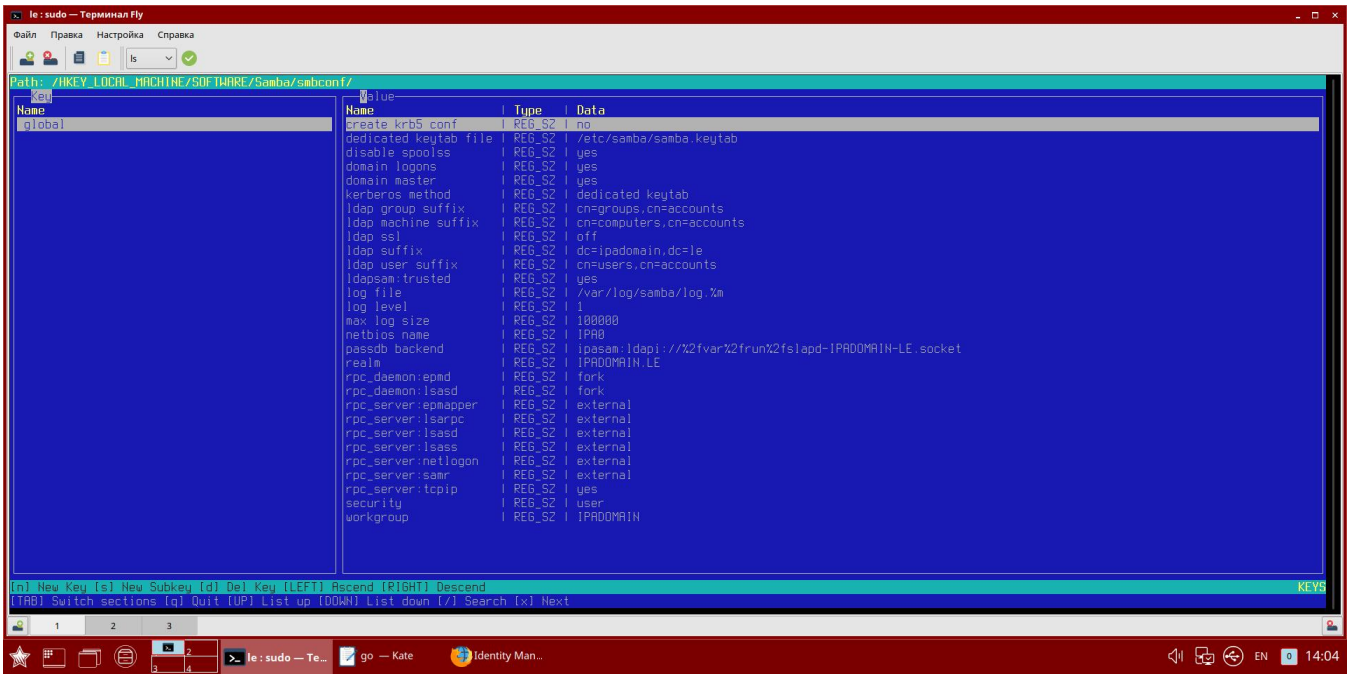
```
sudo testparm
```

Перед редактированием БД "registry" рекомендуем сохранить текущую конфигурацию (вывод команды sudo testparm), чтобы иметь возможность восстановить конфигурацию в случае ошибок.

Редактировать БД "registry" можно с помощью специальной утилиты samba-regedit (устанавливается автоматически при установке пакета samba):

```
sudo samba-regedit
```

При этом параметры samba хранятся в ветке /HKEY_LOCAL_MACHINE/SOFTWARE/Samba/smbconf:




Все секции конфигурационного файла samba (в том числе разделяемые ресурсы, включая специальный ресурс homes) могут быть указаны в этой ветке. Все параметры имеют одинаковый тип REG_SZ.

При этом конфигурационные данные можно импортировать в registry из файлов с синтаксисом конфигурационного файла samba с помощью команды net. Например, создадим разделяемые ресурсы homes и share, для чего:

- Создадим в любом редакторе файл homes.txt с описанием ресурса homes:

```
[homes]
   browseable = no
   comment = Home Directories
   create mask = 0600
   directory mask = 0700
   valid users = %S
# По умолчанию ресурс [homes] предоставляется как ресурс только для чтения (read only = yes).
# Если требуется разрешить запись нужно явно указать read only = no
   read only = No
   guest ok = no
```

- Создадим в любом редакторе файл share.txt с описанием ресурса share:

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

- Импортируем созданные описания ресурсов в конфигурацию samba:

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

После внесения изменений в registry изменения применяются автоматически, и, в отличие от работы с конфигурационным файлом, службу samba перезапускать не нужно.

## Создание домашних каталогов

Для тестирования создадим на сервере условный домашний каталог пользователя admin (т.е. администратора FreeIPA, создаваемого "по умолчанию"):

```
sudo mkhomedir_helper admin
```

## Подключение ресурса с клиентской доменной машины

После выполнения указанных выше действий ресурс (в данном примере - автоматически монтируемый домашний каталог пользователя см. специальный ресурс homes) будет доступен на клиентской машине с авторизацией через Kerberos:

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

## Отдельный сервер Samba

В примере выше сервер Samba запускается непосредственно на контроллере домена. Далее рассмотрим действия по запуску файлового сервера Samba с авторизацией через доменную службу Kerberos на отдельном компьютере. Предполагается, что у нас уже есть работающий контроллер домена ipa0.ipadomain.ru.

1. На контроллере домена:

   Если при установке контроллера домена не была применена опция --setup-adtrust (установка компонент для работы с samba и Windows AD), то доустановить необходимые компоненты:

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

2. На файловом сервере:
    a. Рекомендуется  назначить файловому серверу статический IP-адрес;
    b. Назначить файловому серверу полное доменное имя, например samba.ipadomain.ru:

    ```
    sudo hostnamectl set-hostname samba.ipadomain.ru
    ```

    и в файле /etc/hosts указать настройки IP для этого имени;

    c. Ввести файловый сервер в домен:

    ```
    sudo apt install astra-freeipa-client
    sudo astra-freeipa-client -d ipadomain.ru
    ```

    d. Установить на файловом сервере необходимые пакеты:

    ```
    sudo apt install libwbclient-sssd samba samba-client
    ```

3. После ввода файлового сервера в домен зарегистрировать службу, для чего на контроллере домена выполнить команды:

```
sudo kinit admin
sudo ipa service-add cifs/samba.ipadomain.ru
```

4. После регистрации службы выполнить на файловом сервере
    a. Создание разделяемого файлового ресурса (например /home/share) и назначение ему прав доступа:

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

    b. Получение таблицы ключей:

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

    c. Настройку конфигурации службы samba (файл /etc/samba/smb.conf):

    ```
    [global]
    workgroup = IPADOMAIN
    realm = IPADOMAIN.RU
    dedicated keytab file = FILE:/etc/samba/samba.keytab
    kerberos method = dedicated keytab
    log file = /var/log/samba/log.%m

    [homes]
    browsable = no
    writable = yes

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

    d. Перезапуск службы samba:

    ```
    sudo systemctl restart smbd
    ```

## Ошибки и предупреждения

- Ошибка соединения NT_STATUS_BAD_NETWORK_NAME при попытке доступа к ресурсу говорит о том, что забыли создать на сервере каталог (в данном случае - домашний каталог пользователя).
- Ошибка соединения NT_STATUS_INVALID_PARAMETER при попытке доступа к ресурсу при авторизации Kerberos говорит о том, что неправильно получен билет Kerberos (чаще всего билет получен из-под sudo, а аутентификацию пытаются выполнить без sudo).
- Сообщение "mkdir failed on directory /var/run/samba/msg.lock: Отказано в доступе" на работоспособность клиента Samba не влияет, можно это сообщение убрать на время до следующей перезагрузки системы просто создав на клиентской машине этот каталог командой:

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

  или сделать так, чтобы этот каталог создавался автоматически при загрузке, для чего в файле /usr/lib/tmpfiles.d/samba.conf строчку "d /run/samba 0755 root root -" заменить на строчку "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
  ```

- Сообщение "Unable to initialize messaging context" на работоспособность клиента Samba не влияет.