

# ram\_mount автоматическое монтирование разделяемых ресурсов Samba

- [Введение](#)
- [Установка samba](#)
- [Создание каталогов для общего доступа](#)
- [Конфигурация Samba](#)
  - [Специальный файловый ресурс \[homes\] - домашние каталоги пользователей](#)
- [Подключение разделяемого samba-ресурса в сессии с нулевой классификационной меткой](#)
  - [Монтирование разделяемых файловых ресурсов](#)
  - [Автоматическое монтирование ресурсов при входе пользователя с помощью ram\\_mount](#)
    - [Автоматическое монтирование домашних каталогов при входе пользователя с помощью ram\\_mount](#)



Данная статья применима к:

- ОС ОН Орёл 2.12 (кроме мандатного разграничения доступа)
- ОС СН Смоленск 1.6
- ОС СН Ленинград 8.1

## Введение

Стенд:

- Компьютер-сервер разделяемых ресурсов Samba. В качестве сервера использовался сервер FreeIPA с настройками по умолчанию, т.е. использовалась служба samba, установленная при установке сервера FreeIPA. В примерах далее для этого сервера используется доменное имя **ipa0.ipadomain.ru**.
- Компьютер-клиент. В качестве клиента использовался компьютер, введённый в домен FreeIPA.

## Установка samba

При необходимости установить samba отдельно можно воспользоваться [общей статьёй по настройке Samba](#)

## Создание каталогов для общего доступа

Создать каталоги на сервере, которые будут содержать разделяемые файловые ресурсы и установить желаемые права мандатного и дискретного доступа, например:

Одиночный каталог:

```
sudo mkdir /share1
```

Или, для ОС СН Ленинград/Смоленск, группу каталогов с различным мандатным контекстом:

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

Установить желаемые дискретные атрибуты, например:

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

Разграничить мандатный доступ в соответствии с пунктом "4. МАНДАТНОЕ РАЗГРАНИЧЕНИЕ ДОСТУПА" документа "Руководство по КСЗ. Часть 1 РУСБ.10015-01 97 01-1"[\(ссылка\)](#):

```
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
```

## Конфигурация Samba

Внести в конфигурационный файл `/etc/samba/smb.conf` информацию о разделяемом файловом ресурсе:

#### `/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
```



Для того, чтобы разделяемые samba-ресурсы отображались ресурса в разделе сеть файлового менеджера **fly-fm** с нулевой [классификационной меткой](#) через протокол **NetBIOS** в конфигурационном файле `/etc/samba/smb.conf` должна быть установлена опция "disable netbios = no" (установлена по умолчанию).

```
disable netbios = no
```

После сохранения настроек проверить их корректность

```
testparm
```

Если команда `testparm` не находит ошибок, то перезапустить сервис Samba:

```
sudo systemctl restart smbd
```

Если всё сделано правильно, то команда

```
smbtree
```

покажет название разделяемого ресурса.

## Специальный файловый ресурс `[homes]` - домашние каталоги пользователей

В конфигурации самба зарезервировано имя ресурса `[homes]` - специально обрабатываемое имя для подключения домашних каталогов пользователей. Специальная обработка позволяет подставлять имя пользователя в качестве имени разделяемого ресурса, что удобно для доступа к домашним каталогам.

Хотя этот ресурс по умолчанию указан в конфигурационном файле, для того, чтобы это ресурс можно был использовать необходимо выполнить следующие подготовительные действия:

- Добавить в секцию `[global]` конфигурационного файла параметр

```
i passwd backend = smbpasswd
```

- Перезапустить службу samba

```
sudo systemctl restart smb
```

- Добавить пользователя в список пользователей samba:

```
smbpasswd -a username
```

Описание разделяемого ресурса [homes] в файле /etc/samba/smb.conf может выглядеть вот так:

```
i [homes]
comment = Home Directories
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
create mask = 0700
directory mask = 0700
browseable = no
guest ok = no
```

При этом в описании ресурса может отсутствовать в явном виде указание самого разделяемого каталога, а обращение к такому ресурсу выполняется по имени пользователя (предполагается, что команда smbclient вызвана от имени пользователя username):

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

Или можно явно задать имя пользователя, от имени которого должен вызываться ресурс:

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

При каждом таком обращении samba сначала ищет имя запрошенного ресурса в списке разделяемых ресурсов, и если имя не найдено проверяет наличие в конфигурации секции [homes].

Если такая секция есть, то имя трактуется как имя пользователя, и проверяется по базе данных пользователей (например, /etc/passwd).

Если имя найдено в базе данных пользователей, то samba предоставляет в качестве разделяемого ресурса домашний каталог этого пользователя.

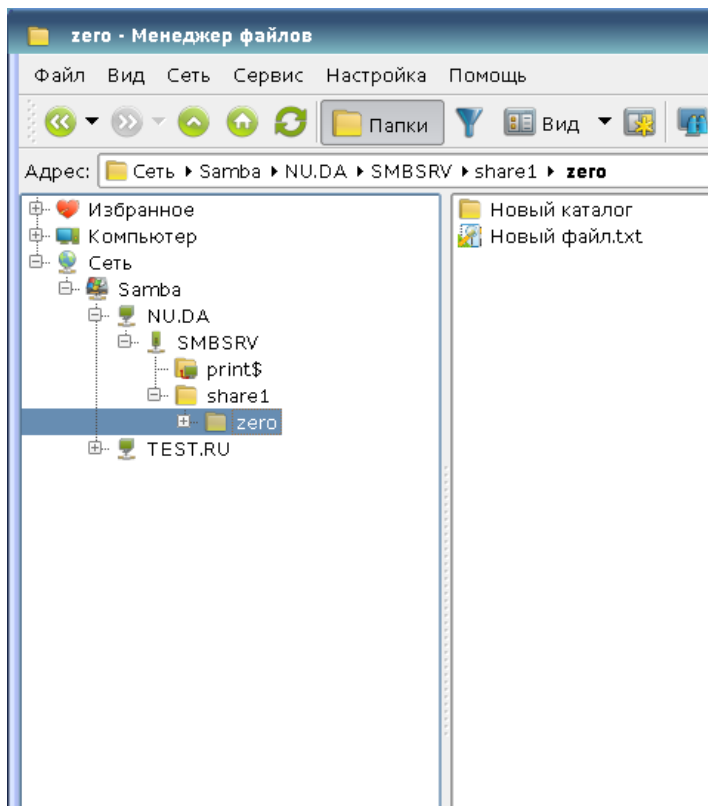
Каталог в простейшем случае берётся из файла /etc/passwd, но может быть [изменён](#).

В качестве дополнительной опции разделяемого ресурса [homes] можно задать параметр path, указывающий путь к корневому каталогу домашних каталогов пользователей, который будет использоваться вместо каталога /home, т.е. будет предоставляться ресурс не /home/username, а, например, /samba/users/username:

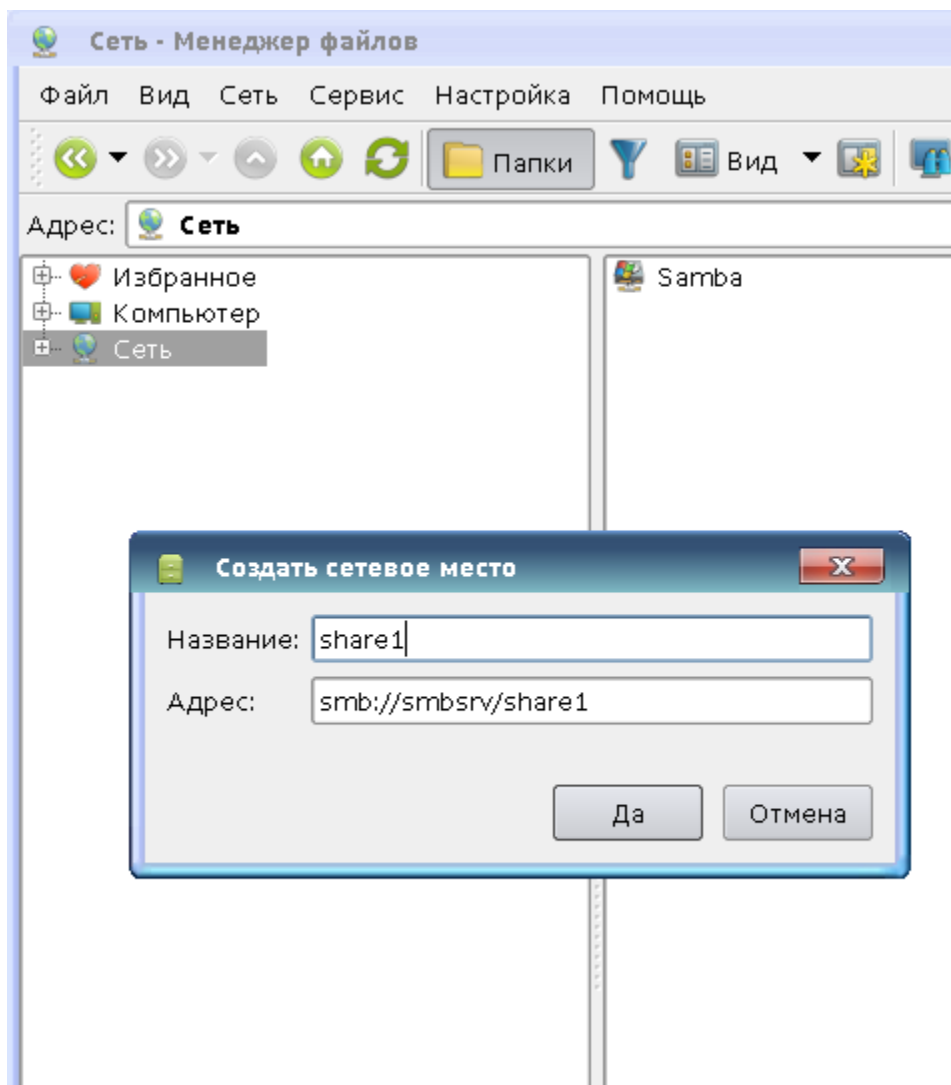
```
i [homes]
comment = Home Directories
valid users = %S
path = /samba/users/%S
read only = No
create mask = 0700
directory mask = 0700
browseable = no
guest ok = no
```

## Подключение разделяемого samba-ресурса в сессии с нулевой классификационной меткой

Запустить менеджер файлов (**fly-fm**) и открыть раздел "Сеть", в котором отобразятся ресурсы **Samba** при условии включенного **NetBIOS** и его видимости:



Если ресурс не виден для других и **NetBIOS** отключен, то его можно добавить самостоятельно, выбрав закладку "Сеть" или правым щелчком по разделу "Сеть":



⚠ При входе с ненулевой классификационной меткой отображение сетевых ресурсов в файловом менеджере fly-fm недоступно.

## Монтирование разделяемых файловых ресурсов

Для монтирования разделяемых файловых ресурсов на компьютере-клиенте должен быть установлен пакет cifs-utils:

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

Монтирование разделяемого файлового ресурса выполняется командой mount с указанием соответствующего типа сетевой ФС, например:

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

В качестве опций команде могут передаваться параметры монтирования, такие как имя пользователя, используемый тип аутентификации, кодировка, использование прав доступа и т.п. При этом точка монтирования `/media/share1` должна быть создана заранее и доступна пользователю, например:

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

Без соответствующей записи в `/etc/fstab` пользователь может использовать команды монтирования только с помощью `sudo`.

Для возможности монтирования разделяемого файлового ресурса пользователем в конфигурационном файле `/etc/fstab` должна быть объявлена строка монтирования, например следующего вида:

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

Точка монтирования должна быть создана заранее и доступна пользователю для чтения/записи, опция `user` предоставляет возможность монтирования указанного ресурса простому пользователю.

Пользователь при этом выполняет монтирование командой `mount` с указанием точки монтирования:

```
mount /media/share1
```


Полный список опций приведен в руководстве `man` для команд `mount` и `mount.cifs`. Описание формата конфигурационного файла `/etc/fstab` приведено в руководстве `man` для `fstab`.

Для того чтобы были пользователю были доступны каталоги при входе с ненулевой классификационной меткой нужно в файле `/etc/fstab` на компьютере клиента указать следующие параметры:

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

#### Примечание


При использовании с аутентификацией Kerberos в ЕПП в строке опций должен быть указан параметр аутентификации `sec=krb5i` или `sec=krb5`. В этом случае при монтировании будет использоваться текущий кэш Kerberos пользователя.

 Для аутентификации через Kerberos должен быть настроен сервер Kerberos, например [FreeIPA](#).  
См. [порядок действий по настройке сервера FreeIPA для предоставления разделяемых ресурсов через Kerberos](#).

## Автоматическое монтирование ресурсов при входе пользователя с помощью `ram_mount`

Для автоматического монтирования разделяемых файловых ресурсов при входе пользователя используется `ram` модуль `pam_mount`, предоставляемый пакетом `libpam-mount`, то есть для автоматического монтирования разделяемых файловых ресурсов на компьютере-клиенте должны быть установлены пакеты `cifs-utils` и `libpam_mount`:

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

 При установке пакета `libpam-mount` может выдаваться предупреждение об изменении конфигурации PAM-стека. Можно согласиться с внесением изменений (после установки следует проверить изменения в каталоге `/etc/pam.d/`, и восстановить нужную конфигурацию).  
Можно отказаться от внесения изменений, тогда вызов модуля `ram_mount` нужно будет внести в `ram`-стек самостоятельно.

Настройка модуля `ram_mount` осуществляется с помощью конфигурационного файла `/etc/security/pam_mount.conf.xml`.

При установке пакета `libpam_mount` вызов модуля `ram_mount` автоматически вносится в соответствующие `pam`-сценарии (`common-auth`, `common-session`) в каталоге `/etc/pam.d`.

Описание возможностей модуля `pam_mount` и формат его конфигурационного файла приведены в руководстве `man` для `pam_mount` и `pam_mount.conf`.

Для монтирования с помощью `ram-mount` разделяемых файловых ресурсов в конфигурационном файле должны быть указаны параметра монтируемого тома, например:

```
/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 -->
<logout wait="50000" hup="1" term="1" kill="1" />
<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),cuid=%(USER),sec=krb5i"
/>

<!--
<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="0" hup="no" term="no" kill="no" />

    <!-- pam_mount parameters: Volume-related -->

<mkmountpoint enable="1" remove="true" />

</pam_mount>

```

**i** В приведённом выше примере разделяемый ресурс при входе любого пользователя монтируется в каталог /media/username. При этом выбраны опции монтирования, позволяющие осуществлять доступ к смонтированным данным в соответствии с правилами мандатного разграничения доступа. Если указать в параметрах тома mountpoint="/home/%(USER)/share1" то разделяемый ресурс будет монтироваться в подкаталог /share1/ домашнего каталога пользователя. В Astra Linux SE (ОС СМ Смоленск/Ленинград) для того, чтобы монтирование корректно выполнялось при входе с ненулевой меткой безопасности, нужно изменить ПАМ-стек, так, чтобы автоматическое монтирование с помощью pam\_mount выполнялось после определения значений мандатных атрибутов пользователя и создания домашнего каталога. Для этого:

1. Вызов модуля pam\_mount удалить из файла /etc/pam.d/common-session;
2. Добавить в файлы /etc/pam.d/login и /etc/pam.d/fly-dm после вызова соответствующих модулей Astra Linux:

Для FreeIPA (добавленная строка выделена жирным шрифтом):

**i** session required pam\_parsec\_mac.so  
**session optional pam\_mount.so**

Для ALD (добавленная строка выделена жирным шрифтом):

**i**


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


- При использовании с аутентификацией Kerberos в ЕПП в строке опций монтирования должен быть указан параметр аутентификации `sec=krb5i` (предпочтительно с точки зрения безопасности, но требует больше ресурсов) или `sec=krb5`. В этом случае при монтировании будет использоваться текущий кэш **Kerberos** пользователя.

### **Внимание**

В строке опций монтирования должен присутствовать параметр `cruid=%(USER)`, поскольку монтирование во время создания сессии выполняется от имени привилегированного пользователя.

Для точки монтирования `mountpoint` должен быть указан отдельный каталог, например: `/media/ald_share`. Пример:

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

 Тег `logout` определяет поведение в процессе размонтирования ФС. К этому времени все процессы должны освободить точку монтирования, в противном случае им посылаются соответствующие сигналы прерывания работы.

Тег `mkmountpoint` отвечает за автоматическое создание и удаление точки монтирования.

Тег `cifsmount` определяет команду, с помощью которой монтируется указанный тип ФС.

Тег `volume` объявляет непосредственно параметры монтирования разделяемого файлового ресурса.

## Автоматическое монтирование домашних каталогов при входе пользователя с помощью `pam_mount`

Для автоматического монтирования используем ресурс `[homes]`. Модифицируем конфигурацию `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 -->
    <logout wait="50000" hup="1" term="1" kill="1" />

    <!-- homes -->
    <cifsmount>mount.cifs //%(SERVER)/%(USER) %(MNTPT) -o %(OPTIONS) </cifsmount>

    <!-- pam_mount parameters: General tunables -->
    <!-- , -->
    <volume
        fstype="cifs"
        server="ipa0.ipadomain.ru"
        path="share1"
    <!-- homes -->
        mountpoint="/home/%(USER)"
        options="rw,user=%(USER),gid=%(USER),uid=%(USER),cruid=%(USER),sec=krb5i"
    />

<!--
```



```
<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="0" hup="no" term="no" kill="no" />

      <!-- pam_mount parameters: Volume-related -->

<mkmountpoint enable="1" remove="true" />

</pam_mount>
```