

Настройка Samba ресурсов

Статья для операционной системы специального назначения "Astra Linux Special Edition" (ОС СН) версии 1.5 и "Astra Linux Common Edition" (ОС ОН) 1.11

- [Создание каталогов для общего доступа](#)
- [Конфигурация Samba](#)
- [Подключение ресурса в сессии не отличной от нуля](#)
- [Монтирование разделяемых файловых ресурсов](#)
- [Автоматическое монтирование ресурсов при входе пользователя с помощью pam_mount](#)

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:

```
mkdir /share1
```

Или группу каталогов с различным мандатным контекстом:

```
mkdir /share1
mkdir /share1/zero
mkdir /share1/dsp
mkdir /share1/secret
mkdir /share1/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"[\(ссылка\)](#):

```
pdpl-file 3:0:-1:ccnr /share1/
pdpl-file 1:0:0 /share1/dsp
pdpl-file 2:0:0 /share1/secret
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 = da.net

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



Для отображения ресурса в разделе сеть файлового менеджера **fly-fm** под меткой не отличной от нуля через протокол **NetBIOS**, установить опцию "disable netbios = no"

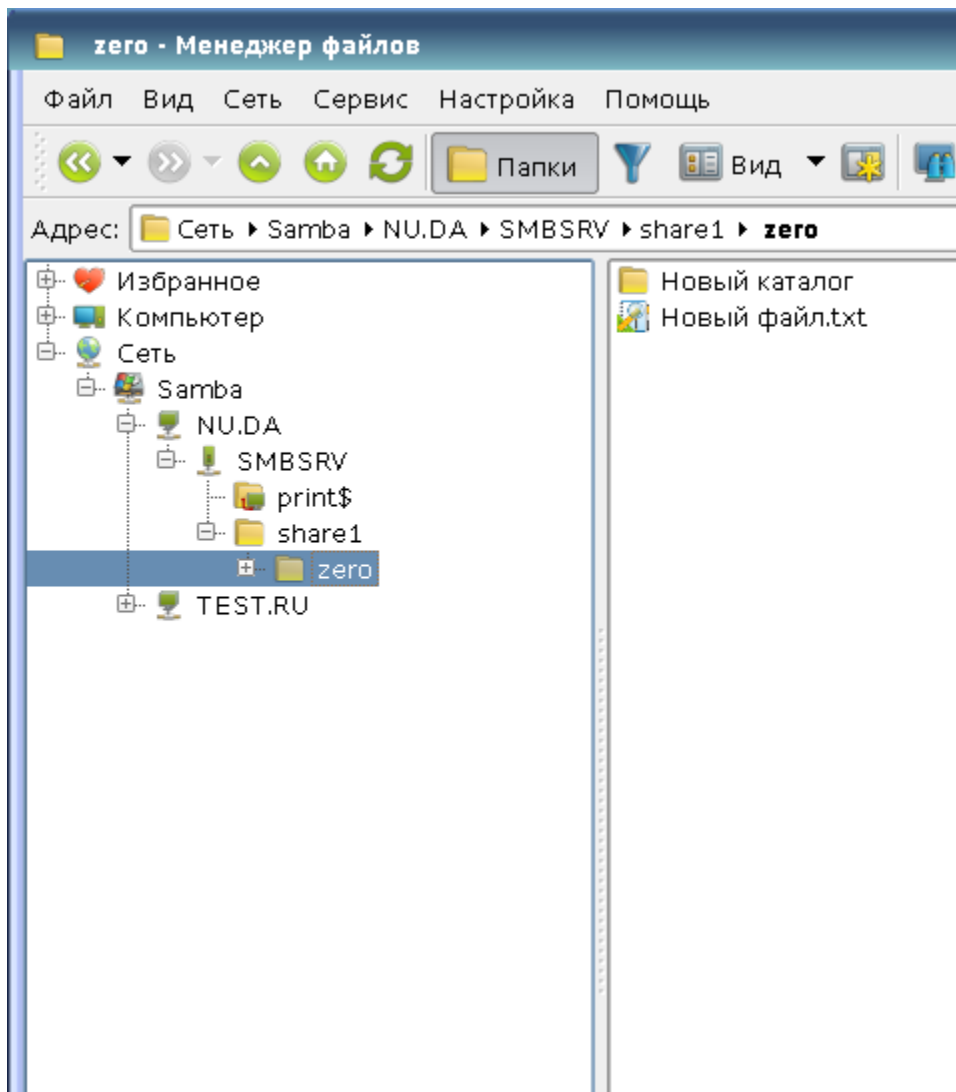
```
disable netbios = no
```

После сохранения настроек перезапустить сервис Samba:

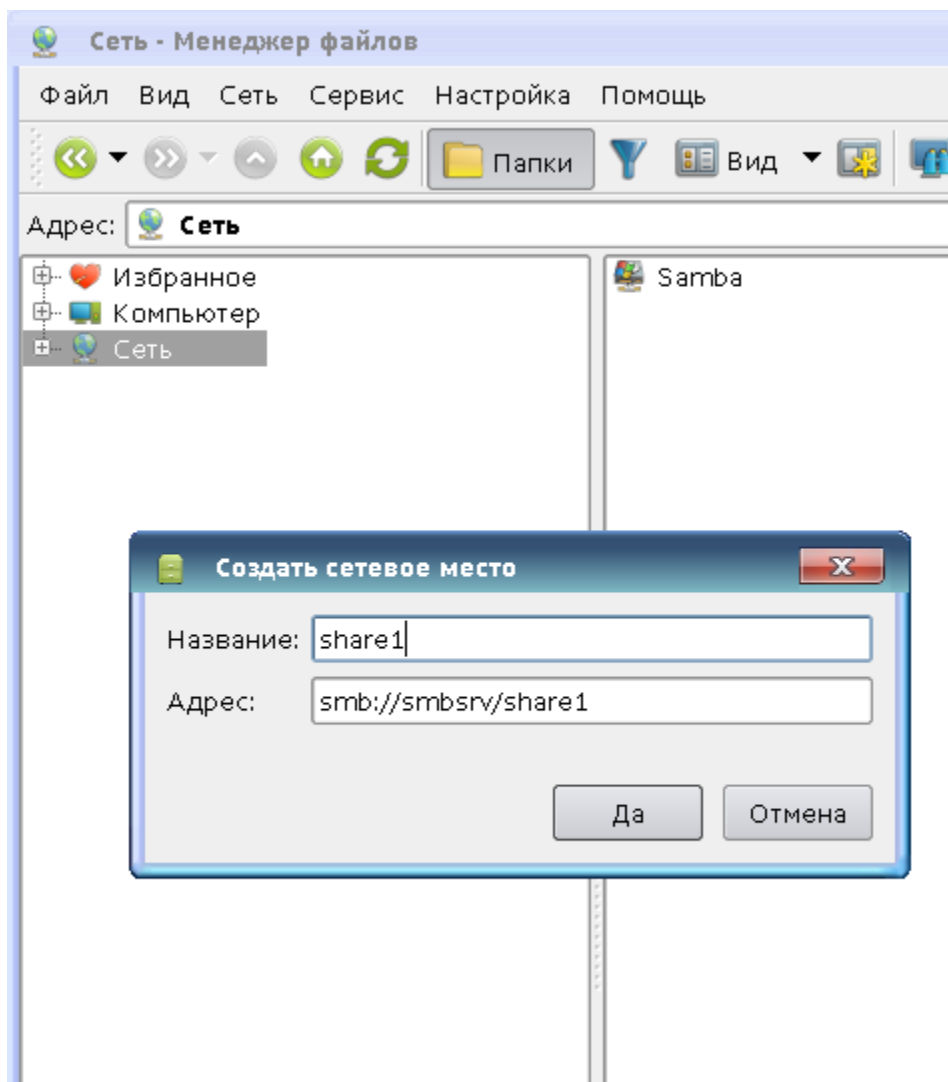
```
service samba restart
```

Подключение ресурса в сессии не отличной от нуля

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":



i Для использования ресурсов **Samba** пользователь должен входить в группу **fuse**

! Начиная с версий ОС ОН Орёл 2.12 и ОС СН Смоленск 1.6 группа fuse не используется

Монтирование разделяемых файловых ресурсов

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

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

Первый вариант команды доступен только суперпользователю.

В качестве опций команде могут передаваться параметры монтирования, такие как имя пользователя, используемый тип аутентификации, кодировка, использование прав доступа и т.п. Полный список опций приведен в руководстве `man` для команд `mount` и `mount.cifs`. Без соответствующей записи в `/etc/fstab` пользователь может использовать команды монтирования только с помощью `sudo` (точка монтирования `~/share1` должна быть создана заранее):

```
sudo mount -t cifs //fileserver1.org.net/share1 ~/share1 -o user=
```

Для возможности монтирования разделяемого файлового ресурса пользователем в конфигурационный файл `/etc/fstab`:

1. Должен быть установлен пакет `cifs-utils`:

```
apt install cifs-utils
```

2. Должна быть объявлена строка монтирования, например следующего вида:

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

3. Точка монтирования должна быть создана заранее и доступна пользователю, опция `user` предоставляет возможность монтирования указанного ресурса простому пользователю. 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`.
4. Для того чтобы были видны каталоги под уровнем `-` в `fstab` на клиенте прописываем следующие параметры:

```
 //fileserver1.org.net/share1 /media/share1 cifs user,rw,noauto,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`. В этом случае при монтировании будет использоваться текущий кэш **Kerberos** пользователя.

Автоматическое монтирование ресурсов при входе пользователя с помощью `pam_mount`

Для автоматического монтирования разделяемых файловых ресурсов при входе пользователя используется `pam` модуль **pam_mount**, предоставляемый пакетом **libpam-mount**, который может быть установлен следующим образом:

```
apt-get install libpam-mount
```

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

Использование **pam** модуля указывается в соответствующих **pam** сценариях (`common-auth`, `common-session`) в каталоге `/etc/pam.d`.

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

Для монтирования с помощью `pam-mount` разделяемых файловых ресурсов **СЗФС CIFS**, представляющих собой домашние каталоги пользователей, конфигурационный файл должен быть модифицирован следующим образом (в пределах тега **pam_mount**):

`/etc/security/pam_mount.conf.xml`

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE pam_mount SYSTEM "pam_mount.conf.xml.dtd">

<pam_mount>

<logout wait="500000" hup="1" term="1" kill="1" />
<mkmountpoint enable="1" remove="true" />
<cifsmount>mount.cifs //%(SERVER)/%(VOLUME) %(MNTPT) -o %(OPTIONS)</cifsmount>
<volume fstype="cifs" server="fileserver1.org.net"
path="homes" mountpoint="[mountpoint_homes]/%(USER)"
options="user=%(USER),rw,setuids,perm,soft,iocharset=utf8" />

</pam_mount>
```

 **Внимание**


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

Так же в строке опций монтирования должен присутствовать параметр `cruid=%(USERUID)`, 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=%(USERUID),iocharset=utf8" />
```

 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. Пользователь должен существовать в БД учетных записей **Samba** и иметь соответствующий пароль.