Samba (Русский)

- Page
- Discussion

- Read
- View source
- View history

Состояние перевода: На этой странице представлен перевод статьи **Samba**. Дата последней синхронизации: 20 марта 2022. Вы можете **помочь** синхронизировать перевод, если в английской версии произошли **изменения**.

Samba — это реализация сетевого протокола **SMB**. Она облегчает организацию общего доступа к файлам и принтерам между системами Linux и Windows и является альтернативой **NFS**.

Ссылки по теме
Интеграция Active Directory
Samba/Контроллер домена Active Directory
NFS (Русский)

Создание общих ресурсов описано в разделе **#Сервер**; подключение к общим ресурсам описано в разделе **#Клиент**.

Сервер

Установка

Установите пакет **samba**.

Samba настраивается с помощью файла `/etc/samba/smb.conf`, который подробно документирован на странице руководства **`smb.conf(5)`**.

В связи с тем, что пакет **`samba`** поставляется без данного файла, вам нужно создать его **перед** запуском `smb.service`.

Вы можете воспользоваться документированным примером, как в `smb.conf.default` из **git-репозитория Samba** для создания `/etc/samba/smb.conf`.

Примечание:

- Значение `log file` в стандартном файле настроек указывает в место, доступное только для чтения, что будет вызывать ошибки. Можно воспользоваться одним из следующих решений:
- Задайте расположение, доступное для записи: `log file = /var/log/samba/%m.log`
- Используйте бекенд для нефайлового журналирования: замените `logging = syslog` на `syslog only = yes` или используйте `logging = systemd`
- Если требуется; `workgroup`, указанная в секции `[global]`, должна соответствовать домашней группе (workgroup) Windows (по умолчанию: `WORKGROUP`).

Совет: Каждый раз, когда вы изменяете файл `smb.conf`, запускайте команду **`testparm(1)`** для проверки файла на синтаксические ошибки.

Включение и запуск служб

Для работы общего доступа к файлам **запустите** и **включите** службу `smb.service`. Смотрите **`smbd(8)`** для более подробной информации.

Если вы хотите, чтобы сервер был доступен по имени хоста NetBIOS, пропишите желаемое имя в опции `netbios name` в `smb.conf` и **запустите** и **включите** службу `nmb.service`. Смотрите **`nmbd(8)`** для более подробной информации.

Примечание: Использовать `nmb.service` необязательно, однако он нужен для подключения к Samba-серверу по имени хоста (например, `smb://hostname/`). Если в вашей сети используются только компьютеры с Windows 10 или новее, также стоит **установить демон WSD**, чтобы Проводник отображал сервер в просмотре сети.

Настройка межсетевого экрана

Если вы используете **межсетевой экран**, не забудьте открыть необходимые порты (как правило, 137-139 + 445). Для получения информации о полном списке портов, смотрите **использование портов Samba**.

Правило UFW

Профиль **Ufw** для SMB/CIFS доступен в стандартной установке UFW в `ufw-fileserver`.

Разрешите Samba, выполнив команду `ufw allow CIFS` от имени root.

Если вы удалили профиль, создайте или отредактируйте файл `/etc/ufw/applications.d/samba`, добавив следующее:

```
[Samba]

title=LanManager-like file and printer server for Unix

description=The Samba software suite is a collection of programs that implements
the SMB/CIFS protocol for unix systems, allowing you to serve files and printers to
Windows, NT, OS/2 and DOS clients. This protocol is sometimes also referred to as
the LanManager or NetBIOS protocol.

ports=137,138/udp|139,445/tcp
```

Затем загрузите этот профиль в UFW, запустив команду `ufw app update Samba` как root.

После этого можно разрешить доступ к Samba, запустив `ufw allow Samba` от имени root.

Служба firewalld

Для настройки **firewalld**, чтобы разрешить Samba в зоне **home**, выполните:

```
# firewall-cmd --permanent --add-service={samba,samba-client,samba-dc} --zone=home
```

Эти три службы таковы:

- `samba`: для общего доступа к файлам.
- `samba-client`: для просмотра общих ресурсов других устройств по сети.
- `samba-dc`: для **контроллера домена Active Directory**.

Параметр `--permanent` сделает изменения постоянными.

Использование

Управление пользователями

В следующем разделе описывается создание локальной (tdbsam) базы данных пользователей Samba. Для аутентификации пользователей и других целей Samba также может быть привязана к домену Active Directory, может сама служить контроллером домена Active Directory или использоваться с сервером LDAP.

Добавление пользователя

Для работы Samba требуется какой-нибудь Linux-пользователь — вы можете использовать существующего пользователя или **создать нового**.

Примечание: Пользователь и группа *nobody* изначально существуют в системе, используются как гостевой аккаунт (`guest account`) по умолчанию и могут быть использованы в ресурсах для общего доступа с опцией `guest ok = yes`, благодаря чему пользователям не понадобится логиниться для доступа к таким ресурсам.

Хотя имена пользователей Samba общие с системными пользователями, Samba использует для них отдельные пароли. Чтобы добавить нового пользователя Samba, воспользуйтесь следующей, заменив `пользователь_samba` на имя нужного пользователя:

```
# smbpasswd -a пользователь_samba
```

Будет предложено задать пароль для этого пользователя.

В зависимости от **роли сервера** может понадобиться изменить **разрешения и атрибуты файлов** для аккаунта Samba.

Если вы хотите разрешить новому пользователю только доступ к Samba-ресурсам и запретить полноценный вход в систему, можно ограничить возможности входа:

- отключить командную оболочку - `usermod --shell /usr/bin/nologin --lock` *`пользователь_samba`*
- отключить вход по SSH - измените опцию `AllowUsers` в файле `/etc/ssh/sshd_config`

См. также **рекомендации по повышению защищённости системы**.

Просмотр списка пользователей

Список добавленных в Samba пользователей можно посмотреть с помощью команды **`pdbedit(8)`**:

```
# pdbedit -L -v
```

Смена пароля пользователя

Чтобы сменить пароль пользователя, используйте `smbpasswd`:

```
# smbpasswd пользователь_samba
```

Создание общего ресурса для анонимных пользователей

1. Создайте пользователя Linux, который будет использоваться для анонимных пользователей Samba:

```
# useradd guest -s /bin/nologin
```

Примечание: Имя пользователя может быть любым допустимым именем Linux, не только "guest". Пользователь не обязательно должен быть пользователем Samba.

2. Добавьте в `/etc/samba/smb.conf`:

```
/etc/samba/smb.conf
...
[global]
security = user
map to guest = bad user
guest account = guest


[guest]
    comment = guest
    path = /tmp/
    public = yes
    only guest = yes
    writable = yes
    printable = no
```

Теперь все анонимные пользователи будут использовать Linux-пользователя `guest` для доступа к каталогам, указанным в `guest.path` (в данном примере `/tmp/`).

Убедитесь, что общие ресурсы корректно настроены в соответствии с секцией *Share Definitions* из **smb.conf.default**.

Включение следования по символическим ссылкам

Важно: Включение опции `follow symlinks` может быть риском для безопасности.

```
/etc/samba/smb.conf
...
[global]
   follow symlinks = yes
   wide links = yes
   unix extensions = no
```

После изменений **перезапустите** службу `smb.service`.

Примечание: При использовании **AppArmor**, если символическая ссылка указывает за пределы домашнего каталога пользователя или **usershare**, понадобится **изменить разрешения в профиле AppArmor**.

Расширенная конфигурация

Создание ресурсов общего доступа от имени обычного пользователя

Примечание: Это опциональная возможность. Можете пропустить этот раздел, если она вам не нужна.

Usershares — это возможность, позволяющая обычным пользователям добавлять, изменять и удалять собственные ресурсы общего доступа.

1. Создайте каталог, в котором будут храниться описания пользовательских общих ресурсов:

```
# mkdir /var/lib/samba/usershares
```

2. Создайте **группу** для пользователей, которые смогут создавать общие ресурсы:

```
# groupadd -r sambashare
```

3. Измените владельца каталога на `root`, а группу на `sambashare`:

```
# chown root:sambashare /var/lib/samba/usershares
```

4. Измените разрешения каталога `usershares`, чтобы только пользователи из группы `sambashare` могли создавать файлы. Эта команда также устанавливает **sticky bit**, благодаря которому пользователи не смогут удалять чужие общие ресурсы:

```
# chmod 1770 /var/lib/samba/usershares
```

Задайте эти переменные в конфигурационном файле `smb.conf`:

```
/etc/samba/smb.conf
[global]
  usershare path = /var/lib/samba/usershares
  usershare max shares = 100
  usershare allow guests = yes
  usershare owner only = yes
```

Добавьте вашего пользователя в группу *sambashare*. Замените `ваше_имя_пользователя` на имя вашего linux-пользователя:

```
# gpasswd sambashare -a ваше_имя_пользователя
```

Перезапустите службы `smb.service` и `nmb.service`.

Завершите сеанс и войдите снова, чтобы применилось добавление новой группы к вашему пользователю.

Если вы хотите предоставить общий доступ к файлам, находящимся в вашем домашнем каталоге, не забудьте задать доступ как минимум на чтение другим пользователям (`chmod a+rX`).

Теперь у вас должна появиться возможность настраивать общий доступ samba, используя графический интерфейс. Например, в **Thunar** или **Dolphin** вы можете нажать правую кнопку мыши на любом каталоге и предоставить для него общий доступ в сети.

Для настройки общего доступа через командную строку используйте одну из следующих команд:

```
# net usershare add имя-ресурса абсолютный-путь [комментарий] [пользователь:{R|D|F}] [guest_ok={y|n}]

# net usershare delete имя-ресурса

# net usershare list wildcard-имя-ресурса

# net usershare info wildcard-имя-ресурса
```

Установка и форсирование прав доступа

Разрешения могут быть применены и к серверу, и к отдельным ресурсам:

```
/etc/samba/smb.conf
```

```
[global]

  ;inherit owner = unix only ; Наследовать владельца родительского каталога для новых файлов и каталогов

  ;inherit permissions = yes ; Наследовать разрешения родительского каталога для новых файлов и каталогов
```

```
  create mask = 0664
  directory mask = 2755
  force create mode = 0644
  force directory mode = 2755
  ...

[media]
  comment = Ресурс, доступный для greg и pcusers
  path = /path/to/media
  valid users = greg @pcusers
  force group = +pcusers
  public = no
  writable = yes
  create mask = 0664
  directory mask = 2775
  force create mode = 0664
  force directory mode = 2775

[public]
  comment = Общий ресурс, в котором archie имеет доступ на запись
  path = /path/to/public
  public = yes
  read only = yes
  write list = archie
  printable = no

[guests]
```

```
  comment = Ресурс, разрешающий чтение и запись всем пользователям
  path = /path/to/guests
  public = yes
  only guest = yes
  writable = yes
  printable = no
```

См. **smb.conf(5)** для более подробной информации о настройке прав доступа.

Ограничение версии протокола для повышения безопасности

Важно: По умолчанию Samba версии 4.11 допускает соединение с использованием устаревшего и небезопасного протокола SMB1. Для этих версий Samba крайне рекомендуется задать опцию `server min protocol = SMB2_02` для защиты от ransomware атак. В Samba 4.11 и новее по умолчанию используется SMB2, так что изменения не требуются.

В файле `/etc/samba/smb.conf` добавьте опции `server min protocol` и `server max protocol` для ограничения используемых версий протокола:

```
/etc/samba/smb.conf
[global]
  server min protocol = SMB2_02
  ; server max protocol = SMB3
```

См. `server max protocol` в **smb.conf(5)** для обзора поддерживаемых протоколов.

Для совместимости со старыми клиентами и/или серверами вам может понадобиться указать `client min protocol = CORE` или `server min protocol`

`= CORE`, но имейте в виду, что это делает вас уязвимым в связи с эксплойтами в SMB1, в том числе к ransomware атакам.

Совет: Используйте `server min protocol = SMB3_00` если хотите использовать только самый новый протокол SMB3, например с клиентами на Windows 8 и новее.

Клиентам, использующим `mount.cifs`, может понадобиться указать правильный `vers=*`, например:

```
# mount -t cifs //SERVER/имя-ресурса /mnt/точка-монтирования -o
username=пользователь,password=пароль,iocharset=utf8,vers=3.1.1
```

Подробнее см. **`mount.cifs(8)`**.

Использование шифрования SMB

Нативное шифрование транспорта SMB доступно с версии SMB 3.0. Среди клиентов, поддерживающих такое шифрование, имеются Windows 8 и новее, Windows Server 2012 новее, smbclient в Samba 4.1 и новее.

Для использования шифрования по умолчанию установите параметр `server smb encrypt` глобально или для отдельных ресурсов. Возможные значения — `off`, `enabled` (значение по умолчанию), `desired` или `required`:

```
/etc/samba/smb.conf
```

```
[global]

  server smb encrypt = desired
```

Смотрите **`smb.conf(5)`** для более подробной информации, особенно разделы *Effects for SMB1* и *Effects for SMB2*.

Совет: При **ручном монтировании** ресурса укажите опцию монтирования `seal` чтобы принудительно включить шифрование.

Отключение общего доступа к принтерам

По умолчанию Samba предоставляет общий доступ к принтерам, настроенным через **CUPS**.

Если вам это не нужно, используйте следующие опции для отключения:

/etc/samba/smb.conf

```
[global]
  load printers = no
  printing = bsd
  printcap name = /dev/null
  disable spoolss = yes
  show add printer wizard = no
```

Запрет определённых расширений файлов в общем ресурсе Samba

Примечание: Использование этой опции влияет на производительность Samba, так как вынуждает проверять все файлы и каталоги на совпадение по мере их сканирования.

Samba предоставляет опцию для блокирования файлов по определённым паттернам, вроде расширений файлов. Её можно использовать для предотвращения распространения вирусов или для того, чтобы пользователи не тратили место на определённые файлы. Более подробную информацию можно найти в **`smb.conf(5)`**.

/etc/samba/smb.conf

```
...
[myshare]
  comment = Private
  path = /mnt/data
  read only = no
  veto files = /*.exe/*.com/*.dll/*.bat/*.vbs/*.tmp/*.mp3/*.avi/*.mp4/*.wmv/*.wma/
```

Увеличение пропускной способности

Важно: Помните, что это может привести к проблемам с подключением и потенциально сломать ваш стек TCP/IP.

Большинству пользователей подойдут настройки по умолчанию. Однако корректное использование 'socket options' может улучшить производительность, но ошибки в настройке также могут и ухудшить её. Проверяйте эффекты, прежде чем вносить какие-либо серьезные изменения.

Читайте **`smb.conf(5)`** прежде чем применять описанные здесь опции.

Эти опции прописываются в файле `/etc/samba/smb.conf` в секции `[global]`.

SMB3 multi-channel может улучшить производительности, однако иногда может испортить данные из-за race conditions. В будущих версиях ситуация может улучшиться:

```
server multi channel support = yes
```

Ограничение времени бездействия полезно для предотвращения исчерпания ресурсов сервера из-за большого количества неактивных подключений:

```
deadtime = 30
```

Использование sendfile улучшает эффективность использования процессора и повышает скорость Samba:

```
use sendfile = yes
```

Установка min receivefile size разрешает zero-copy запись непосредственно из буфера сокета в кэш файловой системы (если доступен). Это может улучшить производительность, но требует тестирования:

```
min receivefile size = 16384
```

Асинхронное чтение/запись файлов может повысить производительность:

```
aio read size = 1

aio write size = 1
```

Увеличение размера буферов приёма/отправки и флаги оптимизации сокетов могут быть полезны для улучшения производительности. Рекомендуется протестировать каждый флаг отдельно, так как они могут вызывать проблемы в некоторых сетях:

```
socket options = IPTOS_LOWDELAY TCP_NODELAY IPTOS_THROUGHPUT SO_RCVBUF=131072 SO_SNDBUF=131072
```

Примечание: Для некоторых опций может понадобиться изменить настройки сетевого интерфейса, см. **Sysctl#Networking**.

Включение доступа для старых клиентов или устройств

Последние версии Samba больше не предлагают старые методы аутентификации и протоколы, которые всё ещё используются некоторыми старыми клиентами (IP-камерами и т.д.). Такие устройства обычно требуют от сервера разрешения

аутентификации NTLMv1 и протокола NT1, известного как CIFS. Чтобы эти устройства работали с последней версией Samba, добавьте эти два параметра в секцию `[global]`:

```
server min protocol = NT1

ntlm auth = yes
```

Для анонимного/гостевого доступа достаточно лишь первого параметра. Если старое устройство использует имя и пароль для доступа, то нужен и второй параметр тоже.

Включение поиска Spotlight

Spotlight позволяет поддерживающим его клиентам (например, MacOS Finder) быстро искать общие файлы.

Установите и запустите **OpenSearch**. Установите **`fs2es-indexer`**AUR, настройте каталоги, которые вы хотите индексировать, в `/etc/fs2es-indexer/config.yml`, и запустите/включите `fs2es-indexer.service` для периодического индексирования.

Измените `smb.conf` как описано в **Samba wiki** и перезапустите `smb.service` для применения изменений.

Клиент

Установите пакет **`smbclient`**, который предоставляет ftp-подобный интерфейс командной строки. Часто используемые команды описаны в **`smbclient(1)`**.

В качестве легковесной альтернативы (без возможности посмотреть список общих ресурсов и т.д.) можно использовать **`cifs-utils`**, который предоставляет команду `/usr/bin/mount.cifs`.

Некоторые **среды рабочего стола** также имеют графический интерфейс для доступа к общим ресурсам и управления ими (смотрите **#Настройка файлового менеджера**).

Примечание:

- **`smbclient`** требует наличия файла `/etc/samba/smb.conf` (смотрите раздел **#Установка**); можно просто создать пустой файл командой `touch`.
- После установки **`cifs-utils`** или **`smbclient`** загрузите **модуль ядра** `cifs` или перезагрузитесь, чтобы не возникало ошибок монтирования.

Просмотр публичных ресурсов для общего доступа

Чтобы вывести список общедоступных ресурсов на сервере:

```
$ smbclient -L hostname -U%
```

Также можно использовать команду `$ smbtree -N`, которая покажет древовидную диаграмму всех общих ресурсов. Она использует широковещательные (broadcast) запросы и потому не рекомендуется для использования в сетях с большим числом компьютеров, но может быть полезна для проверки правильности имён общих ресурсов. Опция `-N` (`-no-pass`) отключает запрос пароля.

Примечание: `smbtree` использует SMB1 и NetBIOS, что означает, что они должны быть включены на стороне сервера, а на стороне клиента нужно добавить `client min protocol = NT1` в `smb.conf`. Без этого `smbtree` ничего не выведет.

Имена хостов NetBIOS/WINS

Клиенты Samba обрабатывают имена хостов NetBIOS автоматически по умолчанию (поведение регулируется опцией `name resolve order` в `smb.conf`). Другие программы (в том числе `mount.cifs`) используют **Name Service Switch**, который не использует NetBIOS по умолчанию.

Пакет **`smbclient`** предоставляет драйвер libnss для разрешения имён NetBIOS. Для его использования **установите** его вместе с пакетом **`samba`** (который предоставляет демон *winbindd*), **запустите** и **включите** службу `winbind.service` и добавьте `wins` в строку `hosts` в файле **`nsswitch.conf(5)`**:

```
/etc/nsswitch.conf
...
hosts: mymachines resolve [!UNAVAIL=return] files myhostname dns wins
...
```

Примечание: Из-за текущей ошибки в `winbind.service` вам нужно вручную изменить файл юнита как описано в **этом баг-репорте**

Теперь в процессе разрешения имён (например, при использовании `mount.cifs` или просто `ping` *`имя-netbios`*) демон *winbindd* будет отправлять запросы с использованием протокола NetBIOS Name Service (NBNS, также известен как WINS).

По умолчанию он отправляет широковещательный (broadcast) запрос в локальную сеть. Если у вас есть WINS-сервер, вы можете добавить `wins server =` *`ip-сервера-wins`* в `smb.conf` и **перезапустить** `winbind.service`, тогда *winbindd* и другие клиенты Samba станут отправлять unicast-запросы на указанный IP.

Если вы хотите, чтобы разрешение имени локального компьютера (которое указывается в опции `netbios name` в `smb.conf`) тоже работало, **запустите** и **включите** службу `nmb.service`, которая будет обрабатывать входящие запросы.

Вы можете протестировать разрешение WINS с помощью `nmblookup`. По умолчанию он отправляет широковещательные запросы в вашу локальную сеть независимо от значения опции `wins server`.

Имейте в виду, что WINS использует трафик, приходящий из порта 137.

Отключение поддержки NetBIOS/WINS

Если разрешение имён хостов NetBIOS/WINS не используется, может быть предпочтительно отключение этого протокола:

/etc/samba/smb.conf

```
[global]

  disable netbios = yes

  dns proxy = no
```

Затем **отключите**/**остановите** `winbind.service`.

Ручное монтирование

Создайте точку монтирования для ресурса:

```
# mkdir /mnt/точка_монтирования
```

Примонтируйте ресурс, в качестве `type` указав `mount.cifs`. Не все опции из перечисленных ниже необходимы или желательны:

```
# mount -t cifs //СЕРВЕР/имя_ресурса /mnt/точка_монтирования -o
username
=имя_пользователя,password=пароль,workgroup=рабочая_группа,iocharset=utf8,uid=польз
ователь,gid=группа
```

Опции `uid` и `gid` соответствуют локальному (клиентскому) пользователю/группе, которые получат доступ на чтение и запись по указанному пути.

Примечание:

- Если используемые `uid` и `gid` не соответствуют пользователю на сервере, могут помочь опции `forceuid` и `forcegid`. Но имейте в виду, что тогда права доступа, отображаемые на клиенте, могут не соответствовать реальным правам доступа на сервере. Подробности смотрите в разделе *File And Directory Ownership And Permissions* в **`mount.cifs(8) § FILE AND DIRECTORY OWNERSHIP AND PERMISSIONS`**.
- Для подключения общего ресурса Windows без аутентификации укажите `"username=*"`.

  Важно: Использование `uid` и/или `gid` может приводить к ошибкам ввода-вывода; вместо этого рекомендуется установить/проверить корректность **разрешений и атрибутов файлов**.
- *`СЕРВЕР`* — Имя сервера.
- *`имя_ресурса`* — Название каталога с общим доступом.
- *`точка_монтирования`* — Локальный каталог, в который будет примонтирован ресурс.

- `[-o опции]` — Смотрите страницу руководства **`mount.cifs(8)`** для получения информации.

  Примечание:

- Не используйте слэш `/` в конце пути. `//СЕРВЕР/имя_ресурса/` не будет работать.
- Если примонтированный вами ресурс работает нестабильно или зависает (freeze), попробуйте включить другую версию протокола SMB, используя опцию `vers=`. Например, `vers=2.0` для Windows Vista.
- Если при завершении работы системы на примонтированных ресурсах происходят таймауты, смотрите **wpa_supplicant#Problem with mounted network shares (cifs) and shutdown**.

  Хранение пароля от общих ресурсов

  Хранение паролей в доступном для чтения файле не рекомендуется. Более безопасным методом является использование файла, например, внутри `/etc/samba/credentials`:

```
/etc/samba/credentials/share
username=имя_пользователя

password=пароль
```

  В команде mount замените опции `username=myuser,password=mypass` на `credentials=/etc/samba/credentials/share`.

  Для безопасности этот файл должен быть доступен только для root:

```
# chown root:root /etc/samba/credentials
```

```
# chmod 700 /etc/samba/credentials

# chmod 600 /etc/samba/credentials/share
```

Автоматическое монтирование

Примечание: Вам может понадобиться **включить** службу `systemd-networkd-wait-online.service` или `NetworkManager-wait-online.service` (зависит от вашей установки) для корректного запуска системы.

С использованием NetworkManager и GIO/gvfs

NetworkManager может быть настроен на запуск скриптов при изменении состояния сети. Приведённый ниже скрипт использует команду *gio*, чтобы автоматически монтировать общие ресурсы Samba аналогично тому, как делает ваш файловый менеджер, как описано **ниже**. Скрипт также безопасно размонтирует их перед отключением сети путём отслеживания событий `pre-down` и `vpn-pre-down`. Сделайте скрипт **исполняемым** после создания.

```
/etc/NetworkManager/dispatcher.d/30-samba.sh
#!/bin/sh


# Найдите UUID нужного соединения с помощью команды «nmcli con show».
# Поддерживаются все типы соединений NetworkManager: беспроводные, VPN, проводные...
WANTED_CON_UUID="CHANGE-ME-NOW-9c7eff15-010a-4b1c-a786-9b4efa218ba9"


# Пользователь, под которым будет примонтирован общий ресурс
USER="yourusername"
```

```
# Путь, который отображается в вашем файловом менеджере, когда вы вручную монтируете нужный общий ресурс
SMB_URL="smb://servername/share"

# Получаем runtime-каталог пользователя. Если его нет, то просто выходим
XDG_RUNTIME_DIR=$(loginctl show-user --property=RuntimePath --value "$USER") || exit 0

if [ "$CONNECTION_UUID" = "$WANTED_CON_UUID" ]; then

    # Параметр скрипта $1: название сетевого интерфейса, не используется
    # Параметр скрипта $2: отправленное событие

    case "$2" in
        "up")
            su $USER -c "DBUS_SESSION_BUS_ADDRESS=unix:path=$XDG_RUNTIME_DIR/bus gio mount $SMB_URL"
            ;;
        "pre-down"|"vpn-pre-down")
            su $USER -c "DBUS_SESSION_BUS_ADDRESS=unix:path=$XDG_RUNTIME_DIR/bus gio mount -uf $SMB_URL"
            ;;
    esac
fi
```

Создайте символическую ссылку в каталоге `/etc/NetworkManager/dispatcher.d/pre-down`, чтобы скрипт получал события `pre-down`:

```
# ln -s /etc/NetworkManager/dispatcher.d/30-samba.sh
/etc/NetworkManager/dispatcher.d/pre-down.d/30-samba.sh
```

Примечание: Так как этот скрипт использует пользовательскую шину, он будет работать, только если у указанного пользователя есть активные сеансы. Это означает, что ресурс не будет примонтирован автоматически после загрузки, если соединение с сетью было установлено до того, как вы залогинились.

С помощью записи в fstab

Простой пример `cifs` **записи в fstab** с аутентификацией:

```
/etc/fstab
//СЕРВЕР/имя_ресурса /mnt/точка_монтирования cifs
_netdev,nofail,username=имя_пользователя,password=пароль 0 0
```

Примечание:

- Пробелы в именах ресурсов должны быть заменены на `\040` (восьмеричный ASCII-код для пробелов). Например, `//СЕРВЕР/имя ресурса` должно быть заменено на `//СЕРВЕР/имя\040ресурса` в `/etc/fstab`.
- Чтобы разрешить монтирование простым пользователям без прав root, когда точка монтирования находится в доступном пользователю каталоге (например, домашнем), добавьте опцию `users` (обязательно с **s** на конце).

Совет: Используйте `x-systemd.automount`, если вы хотите монтировать ресурс только при обращении. Подробнее смотрите **Fstab (Русский)#Автоматическое монтирование с systemd**.

С помощью юнита systemd

Создайте новый файл `.mount` в каталоге `/etc/systemd/system`, например `mnt-myshare.mount`. Смотрите **`systemd.mount(5)`** для более подробной информации.

Примечание: Имя создаваемого файла должно соответствовать точке монтирования, которую вы хотите использовать. Например, имя `mnt-myshare.mount` должно использоваться для точки монтирования `/mnt/myshare`. В противном случае вы получите ошибку `systemd[1]: mnt-myshare.mount: Where= setting does not match unit name. Refusing.`.

`What=` путь к общему ресурсу

`Where=` путь, куда он будет примонтирован

`Options=` опции монтирования

Примечание:

- К сетевым точкам монтирования автоматически добавляются `After`-зависимости `remote-fs-pre.target`, `network.target` и `network-online.target`, а также `Before`-зависимость `remote-fs.target`, если не указана опция `nofail`; иначе используется `Wants`.
- **Добавьте** `noauto` в `Options` для отключения автоматического монтирования (если его не будет монтировать какой-нибудь другой юнит).

- Если в качестве адреса сервера вы хотите использовать имя хоста вместо IP-адреса, добавьте `nss-lookup.target` в `After`. Это может предотвратить ошибки монтироваия при загрузке.

`/etc/systemd/system/mnt-myshare.mount`

```
[Unit]
Description=Mount Share at boot


[Mount]
What=//server/share
Where=/mnt/myshare
Options=_netdev,credentials=/etc/samba/credentials/myshare,iocharset=utf8,rw
Type=cifs
TimeoutSec=30


[Install]
WantedBy=multi-user.target
```

Совет:

- На случай, если удалённая система станет недоступна, **добавьте** `ForceUnmount=true` в секцию `[Mount]`, чтобы разрешить принудительное размонтирование.

- Если общий ресурс имеет группы с доступом только для чтения, **добавьте** `uid=`*`пользователь`* или `gid=`*`группа`* в `Options=`, чтобы указать пользователя/группу, которые имеют право на запись.

Для использования `mnt-myshare.mount` **запустите** этот юнит и **включите** его для автоматического монтирования при загрузке системы.

Автомонтирование

Для автоматического монтирования ресурса (при обращении к нему, как autofs) можно использовать следующий блок automount:

`/etc/systemd/system/mnt-myshare.automount`

```
[Unit]
Description=Automount myshare

[Automount]
Where=/mnt/myshare

[Install]
WantedBy=multi-user.target
```

Остановите и **отключите** юнит `mnt-myshare.mount`, а вместо него **запустите** и **включите** юнит `mnt-myshare.automount`.

Совет: **Добавьте** `TimeoutIdleSec` для включения автоматического размонтирования при бездействии. Подробнее смотрите **`systemd.automount(5)`**.

smbnetfs

Примечание: для smbnetfs необходима целая (нетронутая?) (intact) установка сервера Samba. Смотрите выше, как это сделать

Для начала удостоверьтесь, что вам доступны все ресурсы, которые вам нужны для монтирования:

```
$ smbtree -U удаленный_пользователь
```

Если это не работает, найдите и измените следующую строку в `/etc/samba/smb.conf` подобным образом:

```
domain master = auto
```

Затем **перезапустите** `smb.service` и `nmb.service`.

Если всё работает как нужно, **установите** пакет **`smbnetfs`**.

Затем добавьте следующую строку в файл `/etc/fuse.conf`:

```
user_allow_other
```

Скопируйте каталог `/etc/smbnetfs/.smb` в вашу домашнюю директорию:

```
$ cp -a /etc/smbnetfs/.smb ~
```

Затем создайте ссылку на файл `smb.conf`:

```
$ ln -sf /etc/samba/smb.conf ~/.smb/smb.conf
```

Если для доступа к каким-либо общим ресурсам нужен пароль, измените файл `~/.smb/smbnetfs.auth`, прописав в нём пароли для определённых хостов примерно так:

```
~/.smb/smbnetfs.auth
auth                    "хост" "пользователь" "пароль"
```

Также можно добавить записи для определённых хостов, которые будут монтироваться smbnetfs, если это необходимо. Более подробную информацию можно найти в `~/.smb/smbnetfs.conf`.

Если вы используете **Dolphin** или **GNOME Files**, можно добавить следующую опцию `~/.smb/smbnetfs.conf`, чтобы избежать предупреждений о переполненном диске, так как smbnetfs по умолчанию сообщает, что свободно 0 байт:

```
~/.smb/smbnetfs.conf
free_space_size 1073741824
```

Когда вы закончите настройку, необходимо выполнить

```
$ chmod 600 ~/.smb/smbnetfs.*
```

В противном случае smbnetfs пожалуется: 'insecure config file permissions'.

Наконец, чтобы примонтировать сетевое окружение Samba в каталог по вашему выбору, выполните

```
$ smbnetfs точка_монтирования
```

Демон

Пакет в Arch Linux также поддерживает дополнительный "общесистемный" режим для smbnetfs. Чтобы его включить, вам необходимо выполнить указанные изменения в каталоге `/etc/smbnetfs/.smb`.

Затем вы можете запустить и/или включить в автозагрузку **демон** `smbnetfs` обычным способом. Общесистемной точкой монтирования является `/mnt/smbnet/`.

autofs

Смотрите статью **Autofs** для получения информации об автомонтировщике ядра (kernel-based) Linux.

Настройка файлового менеджера

GNOME Files, Nemo, Caja, Thunar и PCManFM

Чтобы получить доступ к ресурсам samba через GNOME Files, Nemo, Caja, Thunar или PCManFM, установите пакет **`gvfs-smb`**, доступный в **официальных репозиториях**.

Нажмите `Ctrl+l` и введите `smb://`*`имя_сервера`*`/`*`ресурс` в панель адреса, чтобы получить доступ к ресурсу.

Примонтированный ресурс, вероятно, будет представлен в файловой системе по пути `/run/user/`*`ваш_UID`*`/gvfs` или `~/.gvfs`.

KDE

Приложения KDE (например, Dolphin) имеют встроенную возможность просмотра ресурсов Samba, в этом случае нет необходимости в дополнительных пакетах. Используйте адрес `smb://`*`имя_сервера`*`/`*`имя_ресурса` для подключения и просмотра файлов. Для доступа к файлам из приложений, не являющихся частью KDE, можно установить **`kio-fuse`**.

Графический интерфейс настроек предоставляется пакетом **kdenetwork-filesharing**.

Другие графические окружения

Есть несколько полезных программ, но им могут требоваться пакеты, созданные для них. Это может быть сделано с помощью Arch package build system. Хорошая новость заключается в том, что они не нуждаются в особом окружении, устанавливаемом для их поддержки, так что они "тянут" за собой меньше пакетов.

- **pyneighborhood**AUR доступен **AUR**.
- Плагины LinNeighborhood, RUmba, xffm-samba для Xffm недоступен в официальных репозиториях или в **AUR**. Поскольку они не поддерживаются официально (или поддерживаются, но неофициально), они могут быть устаревшими и не работать в полной мере

Советы и рекомендации

Обнаружение общих сетевых ресурсов

Если о других системах в локальной сети ничего не известно, а инструменты вроде **smbnetfs** не подходят, можно попробовать поискать ресурсы Samba вручную.

Сперва **установите** пакеты **nmap** и **smbclient**.

Используйте **nmap** для сканирования локальной сети и поиска систем с открытым TCP-портом 445, который используется протоколом SMB. Имейте в виду, что вам может понадобиться использовать опцию `-Pn` или задать другой **тип пинг-сканирования**, так как Windows-системы обычно защищены межсетевым экраном.

```
$ nmap -p 445 "192.168.1.*"
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-13 12:00 UTC

Nmap scan report for 192.168.1.1

Host is up (0.0011s latency).


PORT    STATE  SERVICE

445/tcp open  microsoft-ds


Nmap scan report for 192.168.1.2

Host is up (0.00011s latency).


PORT    STATE SERVICE

445/tcp open  microsoft-ds


Nmap done: 256 IP addresses (2 hosts up) scanned in 2.45 seconds
```

Первый результат — другая система; второй — клиент, с которого было выполнено сканирование.

Теперь можно подключиться к этим IP-адресам напрямую, но если вы хотите использовать имена хостов NetBIOS, можно использовать **`nmblookup(1)`**, чтобы узнать имена NetBIOS. Имейте в виду, что это не будет работать, если NetBIOS отключен на стороне сервера.

```
$ nmblookup -A 192.168.1.1
```

```
Looking up status of 192.168.1.1

        PUTER           <00> -         B <ACTIVE>

        HOMENET         <00> - <GROUP> B <ACTIVE>
```

```
        PUTER           <03> -         B <ACTIVE>
        PUTER           <20> -         B <ACTIVE>
        HOMENET         <1e> - <GROUP> B <ACTIVE>
        USERNAME        <03> -         B <ACTIVE>
        HOMENET         <1d> -         B <ACTIVE>
        MSBROWSE        <01> - <GROUP> B <ACTIVE>
```

Независимо от вывода, смотрите на **<20>**, который обозначает хост с открытыми сервисами.

С помощью **smbclient(1)** чтобы посмотреть список доступных ресурсов на сервере. Вместо IP-адреса можно использовать NetBIOS-имя (`PUTER` в данном примере), если оно доступно. Если будет запрошен пароль, можно просто нажать Enter — список общих ресурсов всё равно отобразится:

```
$ smbclient -L \\192.168.1.1
Sharename       Type      Comment
---------       ----      -------
MY_MUSIC        Disk
SHAREDDOCS      Disk
PRINTER$        Disk
PRINTER         Printer
IPC$            IPC       Remote Inter Process Communication


Server               Comment
---------            -------
PUTER
```

```
Workgroup            Master

---------            -------

HOMENET               PUTER
```

Удалённое управление компьютером Windows

Samba предлагает набор инструментов для взаимодействия с Windows. Они могут пригодиться, если доступ к компьютеру Windows через удалённый рабочий стол невозможен, как показано на некоторых примерах.

Отправка команды shutdown с комментарием:

```
$ net rpc shutdown -C "comment" -I IPADDRESS -U USERNAME%PASSWORD
```

Принудительное выключение можно вызвать, заменив -C с комментарием на один -f. Для перезапуска можно добавить -r, за которым следует -C или -f.

Остановка и запуск служб:

```
$ net rpc service stop SERVICENAME -I IPADDRESS -U USERNAME%PASSWORD
```

Список доступных команд net rpc:

```
$ net rpc
```

Решение проблем

Не удаётся запустить Samba SMB/CIFS сервер

- Проверьте `smb.conf` на наличие ошибок с помощью **`testparm(1)`**.
- Проверьте корректность прав доступа в `/var/cache/samba/` и **перезапустите** `smb.service`:

```
# chmod 0755 /var/cache/samba/msg
```

Проблемы с разрешениями на SELinux

SELinux по умолчанию не позволяет samba получать доступ к домашним каталогам пользователей. Чтобы решить эту проблему, выполните команду:

```
# setsebool -P samba_enable_home_dirs 1
```

Аналогично, `samba_export_all_ro` и `samba_export_all_rw` дадут доступ к чтению и записи всех файлов.

Проблемы с разрешениями на AppArmor

Если используется путь к ресурсу, расположенному вне домашнего каталога или каталога usershares, внесите его в белый список в `/etc/apparmor.d/local/usr.sbin.smbd`. Например:

```
/etc/apparmor.d/local/usr.sbin.smbd
```

```
"/data/" rk,

"/data/**" lrwk,
```

No dialect specified on mount

Клиент использует неподдерживаемую версию SMB/CIFS, которую сервер не принимает.

Смотрите **#Ограничение версии протокола для повышения безопасности**.

Клиенты Windows продолжают запрашивать пароль, даже если общие ресурсы Samba созданы с правами гостя

Установите опцию `map to guest` в секции `global` в файле `/etc/samba/smb.conf`:

```
map to guest = Bad User
```

С версии Samba 4.10.10 используйте `Bad Password` вместо `Bad User`.

Проблемы подключения к Windows 7 - mount error(12): cannot allocate memory

Известная ошибка Windows 7 "mount error(12): cannot allocate memory" может быть исправлена установкой пары ключей в реестре системы Windows:

- `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache` (установить значение `1`)
- `HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\Size` (установить значение `3`)

В качестве альтернативы можно запустить командную строку от имени Администратора и выполнить следующее:

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v "LargeSystemCache" /t REG_DWORD /d 1 /f

reg add "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /v "Size" /t REG_DWORD /d 3 /f
```

Выполните одно из следующих действий, чтобы изменения вступили в силу:

- Перезагрузите Windows
- Перезапустите службу на сервере через services.msc
- Выполните в командной строке `net stop lanmanserver` и `net start lanmanserver`; после остановки служба может перезапуститься автоматически

  Примечание: Поиск решения в интернете подскажет другое решение, рекомендующее пользователям добавить ключ, изменяющий размер "IRPStackSize". Это неправильное решение для устранения проблемы в Windows 7. Не применяйте его.

  Исходная статья.

Проблемы подключения к Windows 10 1709 и новее - "Windows cannot access" 0x80004005

Эта ошибка затрагивает некоторые машины под управлением Windows 10 версии 1709 и более поздних версий. Она не связана с отключением SMB1 в этой версии, а связана с тем, что Microsoft отключила небезопасный вход для гостей в этой версии для некоторых.

Чтобы исправить ситуацию, откройте редактор групповой политики (`gpedit.msc`). Перейдите к настройке *Конфигурация компьютера\Административные шаблоны\Сеть\Рабочая станция Lanman* > *Включить небезопасные гостевые входы* и включите её. В качестве альтернативы измените следующее значение в реестре:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]

"AllowInsecureGuestAuth"=dword:1
```

Ошибка: Failed to retrieve printer list: NT_STATUS_UNSUCCESSFUL

Если вы являетесь домашним пользователем, используете samba исключительно для организации общего доступа к файлам с сервера или NAS и не заинтересованы в организации общего доступа к принтерам, вы можете исправить эту ошибку, добавив следующие строки в файл `/etc/samba/smb.conf`:

```
/etc/samba/smb.conf
```

```
[global]
  load printers = No
  printing = bsd
  printcap name = /dev/null
  disable spoolss = Yes
```

Перезапустите службу `smb.service` и проверьте журнал:

```
# cat /var/log/samba/smbd.log
```

и больше ошибка не должна появляться.

Не удается предоставить общий доступ к папке

Проблема проявляется в том, что, когда вы пытаетесь предоставить общий доступ к папке через *Dolphin* (файловый менеджер), и вначале, вроде бы, все работает нормально, после перезапуска *Dolphin* иконка ресурса исчезла из папки, а в терминале (*Konsole*) вы видите следующий вывод:

```
‘net usershare’ returned error 255: net usershare: usershares are currently disabled
```

Для решения проблемы включите пользовательские общие ресурсы, как это описано в разделе **#Создание ресурсов общего доступа от имени обычного**

пользователя.

"Просмотр" сети выдает ошибку "Не удалось получить список ресурсов с сервера" (Failed to retrieve share list from server)

И вы используете межсетевой экран (iptables), поскольку не доверяете вашей локальной (школа, университет, отель) сети. Это может происходить по следующей причине: когда smbclient просматривает локальную сеть, он посылает широковещательный запрос на udp-порт 137. Затем серверы сети отвечают вашему клиенту, но, поскольку исходный адрес ответа отличается от адреса назначения, который видел iptables при отправке запроса, iptables не признает ответ как "установленное соединение" ("ESTABLISHED") или "относящийся к запросу" ("RELATED"), и, следовательно, пакет отбрасывается. Возможное решение - добавление:

```
iptables -t raw -A OUTPUT -p udp -m udp --dport 137 -j CT --helper netbios-ns
```

в вашу конфигурацию iptables.

Для **Uncomplicated Firewall** добавьте `nf_conntrack_netbios_ns` в конце следующей строки в `/etc/default/ufw`:

```
IPT_MODULES="nf_conntrack_ftp nf_nat_ftp nf_conntrack_irc nf_nat_irc"
```

и затем выполните следующие команды от имени root:

```
echo 1 > /proc/sys/net/netfilter/nf_conntrack_helper

ufw allow CIFS

ufw reload
```

Чтобы сделать изменения постоянными, добавьте следующую строку в конце файла `/etc/ufw/sysctl.conf`:

```
net.netfilter.nf_conntrack_helper=1
```

protocol negotiation failed: NT_STATUS_INVALID_NETWORK_RESPONSE

Вероятно, клиент не имеет доступа к общим ресурсам. Удостоверьтесь, что IP-адрес клиента прописан в строке `hosts allow =` файла `/etc/samba/smb.conf`.

Также проблема может быть в том, что клиент использует недопустимую версию протокола. Для проверки попробуйте подключиться с помощью `smbclient`, вручную указав максимальную версию протокола:

```
$ smbclient -U <пользователь> -L //<сервер> -m <версия протокола, например SMB2> -W <домен>
```

Если команда выполнится успешно, создайте файл конфигурации:

```
~/.smb/smb.conf
```

```
[global]

  workgroup = <домен>

  client max protocol = SMB2
```

Подключение к серверу завершилось неудачей: (Error NT_STATUS_UNSUCCESSFUL)

Вероятно, вы указываете `smbclient` неправильное имя сервера. Чтобы узнать его, запустите на сервере команду `hostnamectl` и найдите строку "Transient hostname".

Подключение к серверу завершилось неудачей: (Error NT_STATUS_CONNECTION_REFUSED)

Убедитесь, что сервер запущен.

Protocol negotiation failed: NT_STATUS_CONNECTION_RESET

Вероятно, на сервере запрещён SMB1. Добавьте опцию `client max protocol = SMB2` в `/etc/samba/smb.conf`. Или просто добавьте `-m SMB2` к команде `smbclient`.

Правильный пароль не подходит (ошибка 1326)

В **Samba 4.5** аутентификация NTLMv1 по умолчанию отключена. Рекомендуется установить последние доступные обновления на клиентах и запретить доступ для неподдерживаемых клиентов.

Если вам всё ещё нужна поддержка очень старых клиентов без поддержки NTLMv2 (например, Windows XP), можно включить NTLMv1, однако это **не рекомендуется** по соображениям безопасности:

```
/etc/samba/smb.conf
```

```
[global]
  lanman auth = yes
  ntlm auth = yes
```

Если клиенты NTLMv2 не могут пройти аутентификацию при включенном NTLMv1, создайте на клиенте следующий файл:

```
/home/user/.smb/smb.conf
```

```
[global]
```

```
  sec = ntlmv2

  client ntlmv2 auth = yes
```

Это изменение также влияет на общие ресурсы samba, смонтированные с помощью **mount.cifs**. Если после обновления до Samba 4.5 монтирование не удаётся, добавьте опцию **sec=ntlmssp** к команде монтирования, например:

```
mount.cifs //server/share /mnt/point -o sec=ntlmssp,...
```

Смотрите **`mount.cifs(8)`**: **ntlmssp** — Использовать хэширование паролей NTLMv2, заключённое в Raw NTLMSSP сообщении. По умолчанию в основных версиях ядра до версии 3.8 было **sec=ntlm**. В версии 3.8 значение по умолчанию было изменено на **sec=ntlmssp**.

Сопоставление зарезервированных символов Windows

Начиная с ядра 3.18, модуль cifs **по умолчанию использует опцию "mapposix"**. При монтировании ресурса с использованием расширений unix и конфигурации Samba по умолчанию, файлы и каталоги, содержащие один из семи зарезервированных символов Windows `: \ * < > ?`, отображаются, но доступ к ним невозможен.

Возможные решения:

- Использовать недокументированную опцию монтирования `nomapposix` для cifs

```
# mount.cifs //server/share /mnt/point -o nomapposix
```

- Настроить Samba для переадресации символов стиля `mapposix` ("SFM", Services for Mac) на правильные родные символы с помощью **fruit**

```
/etc/samba/smb.conf
```

```
[global]

  vfs objects = catia fruit

  fruit:encoding = native
```

- Написать своё сопоставление запрещённых символов с помощью **catia**

```
/etc/samba/smb.conf
```

```
[global]

  vfs objects = catia

  catia:mappings = 0x22:0xf022, 0x2a:0xf02a, 0x2f:0xf02f, 0x3a:0xf03a, 0x3c:0xf03c,
0x3e:0xf03e, 0x3f:0xf03f, 0x5c:0xf05c, 0x7c:0xf07c, 0x20:0xf020
```

Последний подход (использование catia или fruit) имеет недостаток, заключающийся в фильтрации файлов с непечатаемыми символами.

Папка, к которой открыт доступ через графический интерфейс, недоступна для гостей

Этот раздел предполагает, что:

1. Общие папки настроены, как описано в разделе **#Создание ресурсов общего доступа от имени обычного пользователя**
2. Общая папка создана через графический интерфейс и не пользователем root
3. Включен гостевой доступ для папки
4. Служба Samba перезапускалась с момента последнего изменения файла `/etc/samba/smb.conf`

В качестве примера далее используются следующие значения:

- Общая папка находится внутри домашнего каталога пользователя (`/home/yourUser/Shared`)
- Имя общей папки — *MySharedFiles*
- Гостевой доступ открыт только для чтения.
- Пользователи Windows будут иметь доступ к содержимому общей папки без аутентификации

Проверьте правильность конфигурации samba

Выполните следующую команду из терминала, чтобы проверить правильность настроек:

```
$ testparm
```

Проверьте правильность создания общей папки

Выполните следующие команды из терминала:

```
$ cd /var/lib/samba/usershare

$ ls
```

Если всё хорошо, должен быть файл с именем `mysharedfiles`

Посмотрите его содержимое:

```
$ cat mysharedfiles
```

Содержимое файла должно быть примерно таким:

```
/var/lib/samba/usershare/mysharedfiles
path=/home/yourUser/Shared
```

```
comment=

usershare_acl=S-1-1-0:r

guest_ok=y

sharename=MySharedFiles
```

Проверьте доступ к папке от имени гостя

Выполните следующую команду из терминала. Если будет запрошен пароль, просто нажмите Enter:

```
$ smbclient -L localhost
```

Если всё хорошо, в столбце `Sharename` должен присутствовать MySharedFiles.

Выполните следующую команду, чтобы получить доступ к общей папке в качестве гостя (анонимный вход)

```
$ smbclient -N //localhost/MySharedFiles
```

Если всё хорошо, должно появиться приглашение samba-клиента:

```
smb: \>
```

Проверьте, что гость может посмотреть содержимое папки:

```
smb: \> ls
```

Если появится ошибка `NTFS_STATUS_ACCESS_DENIED`, то проблема скорее всего связана с правами доступа к каталогам Unix. Убедитесь, что пользователь samba имеет доступ к нужной папке и всем родительским папкам. Это можно проверить, войдя в учётную запись нужного пользователя (например, с помощью sudo) и попытавшись перейти в нужный каталог.

Mount error: Host is down

Такая ошибка может появиться при монтировании общих ресурсов Synology NAS. Для решения проблемы используйте опцию `vers=1.0`.

Примечание: SMB1 имеет уязвимости в безопасности и уже использовался в успешных атаках вымогательского ПО.

Software caused connection abort

Файловые менеджеры, использующие **`gvfs-smb`**, могут выдавать ошибку `Software caused connection abort` при записи файла на общий ресурс/сервер. Это может быть связано с тем, что на сервере используется SMB/CIFS версии 1, которую многие маршрутизаторы используют для организации общего доступа к USB-накопителям (например, маршрутизаторы Belkin). Для записи на эти общие ресурсы укажите версию CIFS с помощью опции `vers=1.0`. Например:

```
/etc/fstab
//СЕРВЕР/имя_ресурса /mnt/точка_монтирования cifs
_netdev,guest,file_mode=0777,dir_mode=0777,vers=1.0 0 0
```

Это также может произойти после обновления Samba до версии 4.11, в которой SMB1 отключен по умолчанию. Его можно включить с помощью следующей опции:

```
/etc/samba/smb.conf
[global]

client min protocol = CORE
```

Ошибка аутентификации

Убедитесь в отсутствии пробелов перед именем пользователя в настройках Samba:

```
~/.samba
```

```
username= user

password=pass
```

Правильно так:

```
~/.samba
```

```
username=user

password=pass
```

Windows 1709 и новее не видит сервер samba при просмотре сети

В Windows 10 версии 1511 поддержка SMBv1 и, соответственно, обнаружение устройств NetBIOS были отключены по умолчанию. Более новые версии Windows, начиная с версии 1709 ("Fall Creators Update"), больше не позволяют установить клиент SMBv1. Это приводит к тому, что хосты с Samba не отображаются в просмотре сети в Проводнике. Хотя проблем с подключением нет и Samba будет работать нормально, пользователи могут захотеть, чтобы их хосты Samba всё-таки отображались. **wsdd**AUR реализует демон Web Service Discovery. Благодаря ему (Samba) хосты, такие как NAS, могут быть обнаружены клиентами Web Service Discovery, такими как Windows. Настройки по умолчанию должны работать для большинства установок, и всё, что вам нужно сделать, это **запустить** и **включить** службу `wsdd.service`.

Настройки по умолчанию (представлять себя, используя имя хоста машины и рабочую группу "WORKGROUP") должна подходить в большинстве случаев. Если нужно, вы можете изменить настройки, передав wsdd дополнительные аргументы, добавив их в `/etc/conf.d/wsdd` (подробности есть в руководстве wsdd).

wsdd2AUR делает то же самое, но написан на C, а не на Python. По умолчанию он берёт параметры `netbios name` и `workgroup` из файла `smb.conf`.

Файлы из IOS больше не могут копироваться в общий ресурс Samba в Arch Linux, начиная с IOS 14.5

Начиная с IOS 14.5 при попытке передачи данных с устройства под управлением IOS с помощью приложения "Файлы" на общий ресурс samba в Arch Linux возникает ошибка:

```
The operation couldn't be completed

Operation canceled
```

Чтобы исправить эту проблему, добавьте следующее в секцию `[global]` файла `smb.conf` и **перезапустите** службу `smb.service`: **[1]**

```
## addition for IOS Files transfer-to server

vfs object = fruit streams_xattr
```

Смотрите также

- **Samba: An Introduction**
- **Официальный сайт Samba**
- **Samba 3.2.x HOWTO and Reference Guide** (устаревшая, но всё ещё самая подробная документация)
- **Википедия**
- **Gentoo:Samba/Guide**
- **Debian:Samba/ServerSimple**

- **KSMBD**[**устаревшая ссылка** 2023-06-17 ⓘ] - Сервер ядра linux, реализующий протокол SMB3 в пространстве ядра для обмена файлами по сети.
- **Ускорение работы Samba**