- Новости
- Программирование
- информационная безопасность
- Веб-разработка
- Научно-популярное
- android
- Текучка
- javascript
- Железо
- управление проектами
- Google
- diy или сделай сам
- гаджеты
- разработка
- космонавтика
- Песочница
- системное администрирование
- Медиа
- будущее здесь
- linux

## Из архивов

- 2016-07-22 09:08:04
  Security Week 29: утечка на форуме Ubuntu, прокси-уязвимость в PHP, Go и Python, 276 заплаток Oracle
- 2016-06-24 18:36:00
  В игровых тестах производительность видеокарты Radeon RX 480 близка к R9 Fury и GeForce GTX 980
- 2016-05-26 14:04:37
  Microsoft отказалась от трюка с обновлением до Windows 10, начинавшемся по закрытию всплывающего окна
- 2016-02-05 07:21:15
  7 способов избавиться от всего лишнего и получать от жизни больше удовольствия (часть 2)
- 2015-12-22 09:00:40
  Безопасность — превыше всего. Последние наработки для Google Chrome

- 2015-11-10 15:36:20
  Яндекс.Маркет из-за сбоя списал лишние деньги с интернет-магазинов
- 2015-09-11 18:29:00
  Платформа Qualcomm Snapdragon Flight призвана упростить и унифицировать разработку электроники дронов потребительского сегмента
- 2015-08-28 17:33:23
  Улицу в Рейкьявике назвали в честь Дарта Вейдера
- 2015-08-28 06:57:06
  [Запуск успешен] Где посмотреть первый после майской аварии запуск «Протона»
- 2015-08-26 18:36:10
  Тайное становится явным, или Драматическая история миллионов адюльтеров

## Обсуждаемое

- Дима к записи WS2812 и STM32Cube
- Dima к записи Смартфон Oukitel U15S может получить ОС Android 7.0
- Леон к записи Trade.com — или куда деть деньги если они жмут карман
- Fantana к записи Как заработать максимум на своем сайте. 22 способа и 240+ ссылок
- Viktor2312 к записи Всем нолям ноль: почти все языки программирования делают это
- Юра к записи «Воскрешаем» HDD с помощью Arduino
- Лев Багин к записи Восстановление данных из внутренней памяти на Android для чайников
- Олеся к записи Опыт эвалюации дипломов в США (WES)
- Сергей к записи Дешевая STM32 плата + Arduino IDE
- иии к записи JsTree — деревья это так просто

## Архивы

- Декабрь 2016 (1593)
- Ноябрь 2016 (2441)
- Октябрь 2016 (2400)
- Сентябрь 2016 (2464)
- Август 2016 (2079)
- Июль 2016 (2197)
- Июнь 2016 (2306)
- Май 2016 (2381)
- Апрель 2016 (2815)
- Март 2016 (2884)


Наверх

# Samba4 в роли AD + файловый сервер

**2014-03-18 в 7:46, admin**, рубрики: active directory, file server, glusterfs, howto, linux, NAS, nix, samba, samba4, SLES 11, windows, домены, метки: active directory, file server, glusterfs, howto, linux, NAS, nix, samba, samba4, SLES 11, windows, мануал
0

В этой статье я рассмотрю по шагам подготовку к использованию Samba4 в роли контроллера домена вкупе с дополнительным файловым сервером так же на базе Samba4. Что в итоге мы получим? Два настроенных сервера с samba4, первый в роли domain controller, второй в роли member server с файлами пользователей. Функционирования этой связки я добивался около месяца, за сим, не поделится конечным рецептом просто не имею права…

:много предыстории: в компании используется файловый сервер на базе samba3.6 с LDAP Backend,
рый содержит список всех пользователей и групп с правами доступа. Права доступа на каталоги
авляются с помощью xattr_acl (Extended file attributes), в LDAP хранится список пользователей с
ветствием группам доступа. Собственно требуется переехать с этой инфраструктуры на samba4…

дготавливаем два сервера для samba4, я использую дистрибутив SUSE Linux Enterprise 11 Service
3 (SLES11 SP3) как корпоративный стандарт, поэтому разворачивать все буду именно на его базе.
е можно собрать самбу из исходников, это по желанию, я же использую готовую сборку от sernet,
рую можно бесплатно получить просто зарегистрировавшись на портале — Portal Enterprise Samba

t производит сборку самбы для нескольких дистрибутивов — Debian, Ubuntu, RHEL, CentOS,
S, openSUSE.
пользовал Samba4 версии 4.1.6

первом сервере, который у нас выступит в роли DC, устанавливаем sernet-samba-ad. Если
икнут проблемы, можно заглянуть в официальную инструкцию — Samba AD DC HOWTO.
бываем прописать имя нашего будущего домена в своем DNS сервере с указанием на наш новый
ер.

е выполняем создание домена с помощью samba-tools.

```
a-tool domain provision --use-rfc2307 --interactive
```

ема запросит несколько параметров, которые необходимо указать, например такие как имя домена
., а так же попросит задать пароль. Собственно только имя домена и нужно указать, все остальные
осы можно оставить с ответами по умолчанию. Пароль администратора должен соответствовать
стандартным политикам паролей в Windows, т.е. иметь как минимум одну маленькую и одну большую
буквы, а так же цифры, плюс минимум 8 символов.

Копируем вновь сконфигуренный самбой конфиг Kerberos в место по умолчанию.

```
cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

Для проверки верной работы Kerberos можно установить krb5-client и проверить работу аутентификации.

```
kinit administrator@EXAMPLE.COM
klist
```

klist должен показать информацию по тикетам, если все ок — идем дальше.

Нужно подправить файл /etc/default/sernet-samba
Правим строчку SAMBA_START_MODE= на следующую.

```
SAMBA_START_MODE="ad"
```

После этого можно запускать саму самбу

```
/etc/init.d/sernet-samba-ad start
```

Если запуск прошел удачно можно считать, что наш контроллер домена уже развернут.

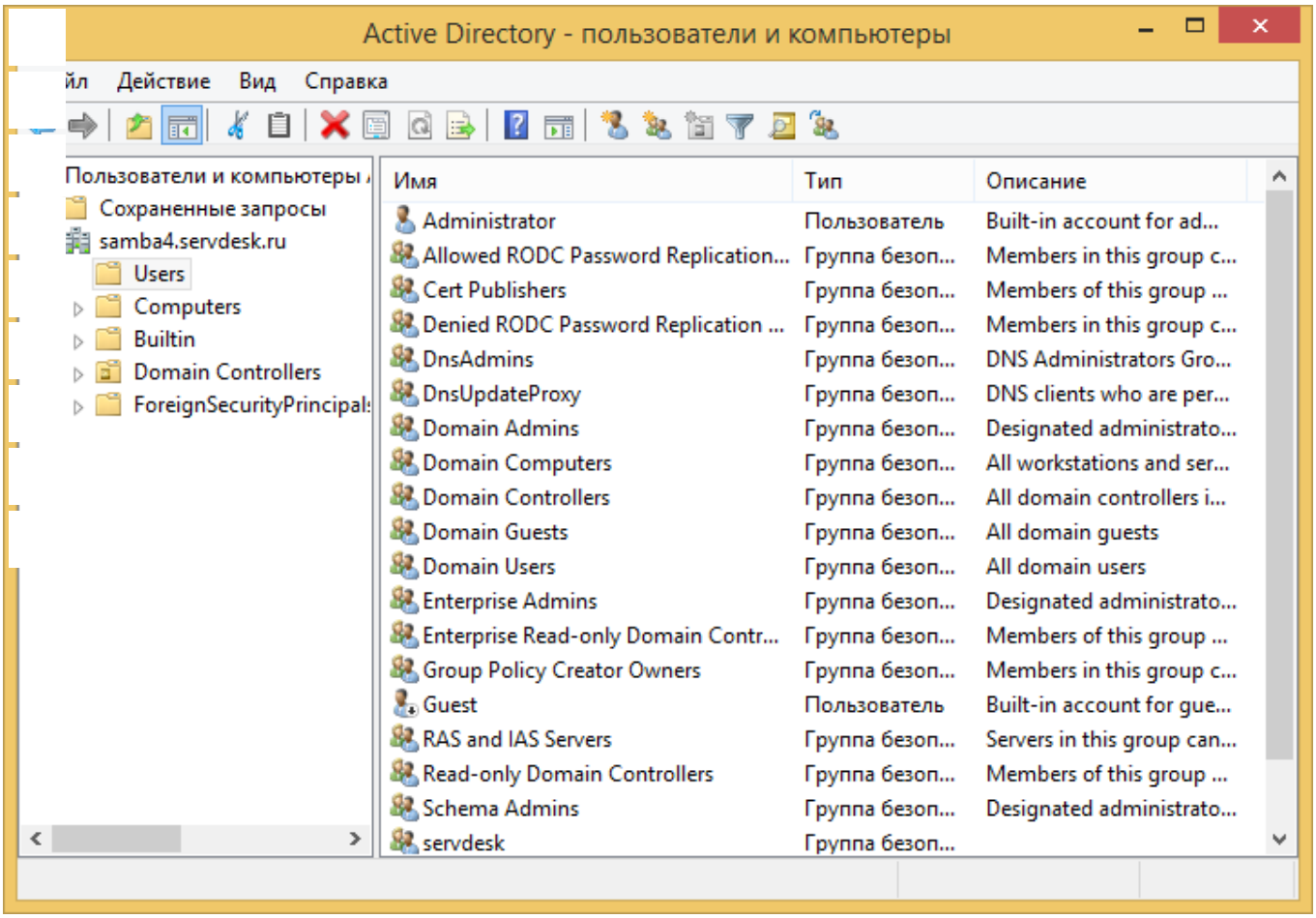
Редактируем файл /etc/nsswitch.conf для того, что бы система увидела пользователей домена и группы, а так же могла нормально выставлять права на файлы. Приводим эти две строки к следующему виду:

```
passwd: compat winbind
group:  compat winbind
```

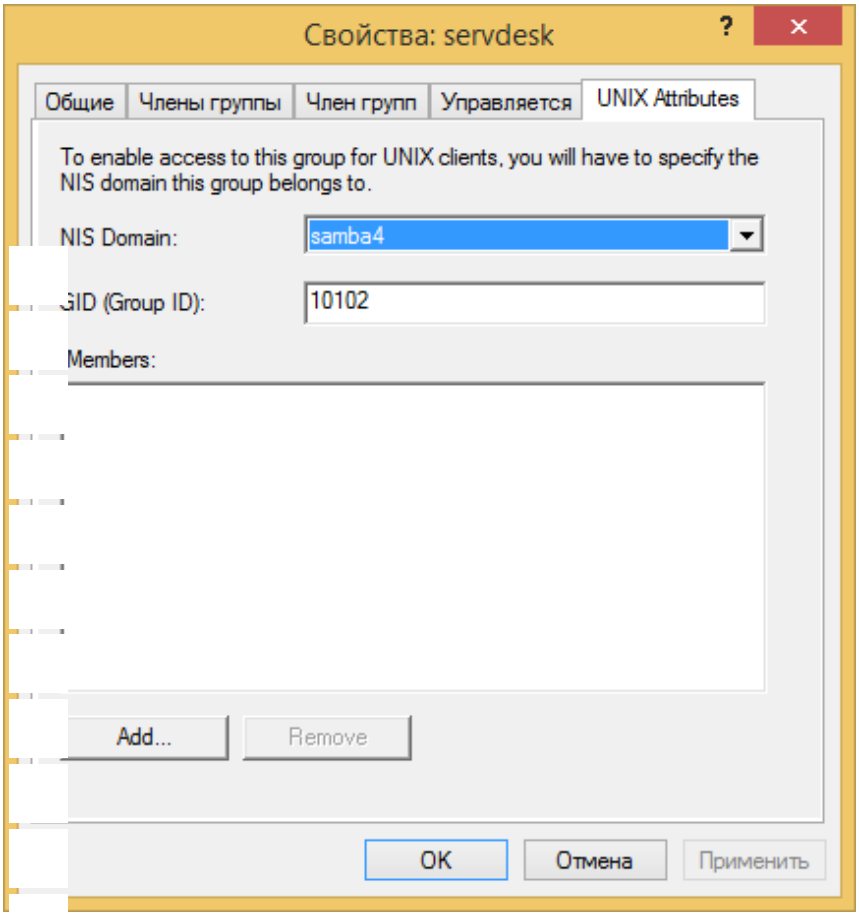
Перезапустим систему и проверим, работает ли… с помощью getent passwd и getent group. Мы должны увидеть группы и пользователей из нашего домена. Более подробно про этот шаг можно почитать официальную инструкцию — Samba4/Winbind

Осталось ввести в домен любую машину с Windows для администрирования, думаю с этим проблем не возникнет.

На машине с Windows, которую мы ввели в домен устанавливаем admin pack. Используем оснастку для управлению пользователями в AD.




Каждой группе и пользователю нужно присвоить unix uidgid для будущей нормальной работы xattr_acl на нашем втором сервере.




Перед тем как начать готовить наш второй сервер, который выступит в роли member server и будет являться файловым сервером в домене.

Устанавливаем sssd, в стандартном репозитории SLES11 имеется версия 1.9.4, она нам вполне подойдет. Так же устанавливаем sssd-tools. sssd нужен для получения пользователей с unix атрибутами с контроллера домена. Более подробно про настройку можно почитать в официальной инструкции — [Local user management and authentication/sssd]
Мы будем настраивать связь с AD через Kerberos.

На первом сервере (DC) нужно экспортировать keytab из Kerberos.

```
samba-tool domain exportkeytab /etc/krb5.sssd.keytab --principa
chown root:root /etc/krb5.sssd.keytab
chmod 600 /etc/krb5.sssd.keytab
```

Для безопасности обрубим лишние права. Копируем keytab файл на наш второй сервер по этому же пути.

Редактируем sssd.conf

```
[sssd]
services = nss, pam
config_file_version = 2
domains = default

[nss]

[pam]

[domain/default]
ad_hostname = smbad.samba4.servdesk.ru
```

```
ad_server = smbad.samba4.servdesk.ru
ad_domain = samba4.servdesk.ru

ldap_schema = rfc2307bis
id_provider = ldap
access_provider = simple

# on large directories, you may want to disable enumeration for performance reasons
    enumerate = true

    auth_provider = krb5
    chpass_provider = krb5
    ldap_sasl_mech = gssapi
    ldap_sasl_authid = smbad$@SAMBA4.SERVDESK.RU
    krb5_realm = SAMBA4.SERVDESK.RU
    krb5_server = smbad.samba4.servdesk.ru
    krb5_kpasswd = smbad.samba4.servdesk.ru
    krb5_keytab = /etc/krb5.sssd.keytab
    krb5_init_creds = true

    ldap_referrals = false
    ldap_uri = ldap://smbad.samba4.servdesk.ru
    ldap_search_base = dc=samba4,dc=servdesk,dc=ru

    dns_update=false

    ldap_id_mapping=false

    ldap_user_object_class = user
    ldap_user_name = samAccountName
    ldap_user_uid_number = uidNumber
    ldap_user_gid_number = gidNumber
    ldap_user_home_directory = unixHomeDirectory
    ldap_user_shell = loginShell

    ldap_group_object_class = group
    ldap_group_name = cn
    ldap_group_member = member
```

l абудьте исправить имя вашего DC и вашего домена на свои. Ставим sssd в автозапуск, перезагружаем сервер.
Далее можно сбросить кеш и проверяем наши группы с пользователями.

```
sss_cache -UG
getent group
...
Schema Admins:*:10110:Administrator
Domain Users:*:10103:
DnsAdmins:*:10117:
servdesk:*:10102:test
```

В списке должны быть наши группы и пользователями с uidgid, которые мы задавали в AD остнастке в Windows.

5) Переходим к настройки samba4 на втором сервере, устанавливаем sernet-samba-nmbd, sernet-samba-smbd, sernet-samba-winbind и все зависимости для них. Более подробно про настройку можно почитать в официальной инструкции — Samba/Domain Member

Создаем smb.conf, мой файл выглядит вот так:

```
[global]

   workgroup = SAMBA4
   security = ADS
   realm = SAMBA4.SERVDESK.RU

#   map untrusted to domain = Yes
```

```
   idmap config *:backend = tdb
   idmap config *:range = 70001-80000

#   idmap config SAMBA4:default = yes
   idmap config SAMBA4:backend = ad
   idmap config SAMBA4:schema_mode = rfc2307
   idmap config SAMBA4:range = 500-40000
    idmap_ldb:use rfc2307 = yes




    winbind nss info = rfc2307
    winbind trusted domains only = no
    winbind use default domain = yes
    winbind enum users  = yes
    winbind enum groups = yes

   ate mask = 0777
   ectory mask = 0777

    objects = acl_xattr btrfs
 acl inherit = Yes
   e dos attributes = Yes


  a1]
   ath = /data1/
   ead only = no
```

Не забываем подправить конфиг под себя, нужно сменить имя домена на ваш.

Теперь наш файл hosts в нем необходимо прямо указать имя нашего member server, иначе зоны DNS не будут автоматически обновляться в AD.

```
    0.0.1       localhost
    0.0.1       samba3.samba4.servdesk.ru       samba3
```

Запустим процедуру входа в наш домен.

```
net ads join -U administrator
```

Потребуется ввести пароль администратора.

Собственно после этого наш member server уже находится в домене.
Можно попробовать с Windows машины подключится на него под своим логином паролем и создать какую-нибудь папку, для проверки прав…
Создали папку 123, проверяем права.

```
getfacl /data1/123

# file: data1/123
# owner: test
# group: Domain40Users
user::rwx
user:test:rwx
group::r-x
group:servdesk:rwx
group:Domain40Users:r-x
mask::rwx
other::r-x
default:user::rwx
default:user:test:rwx
default:group::r-x
default:group:servdesk:rwx
```

```
default:group:Domain40Users:r-x
default:mask::rwx
default:other::r-x
```

Как видим, все права верно выставляются.

Далее можно начинать перенос пользователей в наш новый домен, а так же выставлять права на папки в
с зетствии с вашими пожеланиями.
Т ке можно использовать glusterfs вкупе с samba4 для создания отказоустойчивого файлового сервера,
и о уже совсем другая история…

I у кого-то есть вопросы, буду рад оказать помощь.

Версия для печати

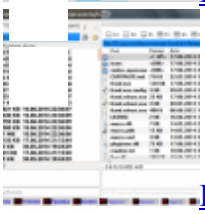
*Автор: AbyssMoon* *Источник*

## Поделиться новостью



## С етуем прочесть:


BITcommander — ваш следующий файловый менеджер


Кросс-платформенный файловый менеджер? Это реальность


Конференц-мост, сервер записи разговоров и Fax-сервер от Grandstream: обзор


Старая печатная машинка с Arduino и Raspberry Pi в роли принтера

Chop-Syc — планшет в роли разделочной доски

Язык программирования и база данных Q: в энтерпрайсе синтаксис роли не играет

* Ваше имя*

Ваш e-mail (не отображается в списке сообщений)

бязательные к заполнению поля

равить!

*ыдущая страница* *Следующая страница*

**ости**

Giada F105D — промышленный безвентиляторный мини-ПК на основе процессоров Intel Apollo Lake
Наушники Apple AirPods способны пережить кратковременное погружение в воду
Apple не будет менять аккумуляторы в наушниках AirPods, потому что их невозможно разобрать и починить

- Моноблоки Acer Aspire C стоят немного, но и оснащены соответственно
- HTC готовит какой-то большой анонс 12 января
- ФРИИ рассказал о двух сорвавшихся сделках на 250 млн рублей — с Group-IB и «Сердитым гражданином»
- Сетевое хранилище Qnap ES1640dc v2 получило шесть портов 10Gbps Ethernet
- Роботы — будущее войн?

**Актуальные темы**

.net android apple c++ css e-commerce Facebook Google html5 iOS iPhone java javascript linux microsoft nokia open source PHP python Samsung windows Windows 8 windows phone Вконтакте Госвеб Нам пишут Онлайн-медиа Программирование Россия Текучка безопасность игры инвестиции кадры кейсы медиа мобильные приложения НОВОСТИ разработка советы социальные сети стартапы статистика телеком яндекс

**Архив**

- Декабрь 2016 (1593)
- Ноябрь 2016 (2441)
- Октябрь 2016 (2400)
- Сентябрь 2016 (2464)
- Август 2016 (2079)
- Июль 2016 (2197)
- Июнь 2016 (2306)

- Май 2016 (2381)
- Апрель 2016 (2815)
- Март 2016 (2884)