Функционал обычного файлового сервера неизменно остается одним из самых популярных и востребованных в работе среднестатистического офиса. Сегодня я расскажу как установить и настроить файловый сервер Samba с авторизацией в AD и управлением доступом с помощью доменных учетных записей. Сразу скажу, что тема это достаточно трудная и хрупкая, очень часто что-то идет не так, нужно неплохо ориентироваться в теме, чтобы решать возникающие проблемы.

> Если у вас есть желание научиться строить и поддерживать высокодоступные и надежные системы, рекомендую познакомиться с **онлайн-курсом «Администратор Linux»** в OTUS. Курс не для новичков, для поступления нужно пройти .

Содержание:

> Прежде чем начинать настройку файлового сервера samba, прочитайте полностью материал, чтобы решить, каким способом будете настраивать. По ходу написания статьи у меня получились 2 принципиально разных решения.

Введение

Ранее я рассказывал как сделать очень простую и быструю настройку самбы, когда доступ ограничивается либо внутренними пользователями самбы, либо с помощью ip. Если вас такой формат эксплуатации файлового сервера устраивает, то читать дальше не обязательно. Используйте приведенную статью, и у вас все получится очень быстро.

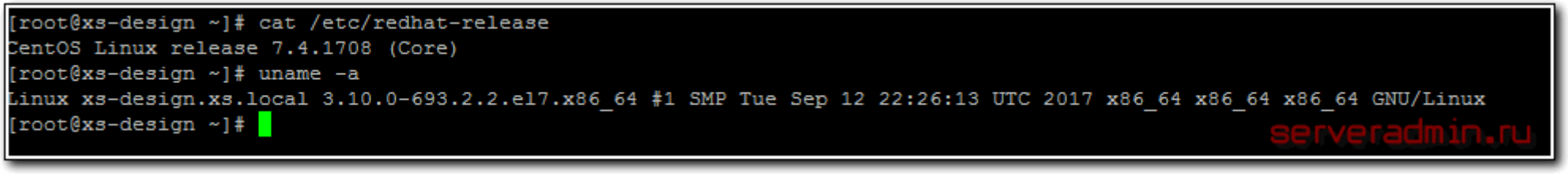
Для более сложной настройки самбы с авторизацией в Active Directory будем разбираться дальше. Существует как минимум 2 способа добавления linux сервера в домен Windows Server:

- Использовать известное и универсальное средство **winbind**.
- Либо воспользоваться менее популярным, но как мне кажется, более удобным и простым в настройке — **sssd**.

Пример добавления linux сервера в домен с помощью winbind я приводил в одной из своих статей по настройке sams с авторизацией в AD. Утилиту sssd я использовал, когда настраивал авторизацию в linux с помощью доменный учетных записей. В этой статье я воспользуюсь sssd для интеграции в виндовый домен.

Если у вас еще нет готового сервера, то можете воспользоваться моими материалами на эту тему — установка и настройка centos 7. Так же рекомендую настроить iptables для корректной работы сервера с доменом windows. Далее я не буду касаться этого вопроса, мы просто отключим фаерволл, потому что его настройка не тема этой статьи.

Настраивать файловую шару samba будем на сервере под управлением CentOS 7 следующей версии:



Вводные слова я все сказал. Начнем настройку самбы с ввода сервера в домен.

Добавляем сервер к домену через realm

Я не буду придумывать ничего нового, а полностью воспользуюсь инструкцией из приведенной выше статьи по настройке авторизации доменных учеток на сервере, но при этом не буду настраивать саму авторизацию. В данном случае мне это не нужно.

Итак, отключаем firewall и SELinux, если не сделали это раньше. Если не хотите отключать, то настройте сами. Данная настройка выходит за рамки статьи.

```
# mcedit /etc/sysconfig/selinux
```

меняем значение

```
SELINUX=disabled
```

Выполняем команду, чтобы не ждать перезагрузки для применения изменений.

```
setenforce 0
```

Выключаем firewalld.

```
# systemctl stop firewalld
# systemctl disable firewalld
```

Информационная таблица

xs.local	название домена
10.1.3.4	ip адрес контроллера домена
xs-winsrv.xs.local	полное имя контроллера домена
xs-design	имя сервера centos, который вводим в домен
admin51	учетная запись администратора домена

> Перед дальнейшей настройкой, убедитесь, что с вашего сервера centos вы без проблем пингуете и резолвите контроллер домена по полному имени. Если есть какие-то проблемы, исправьте это либо указанием нужного dns сервера, либо правкой файла hosts.

Настроим синхронизацию времени с контроллером домена. Это важно, у вас должно быть одинаковое время с контроллером домена. Проверьте его и убедитесь, что стоят одинаковые часовые пояса.

Устанавливаем утилиту для синхронизации времени **chrony**:

```
# yum install chrony
```

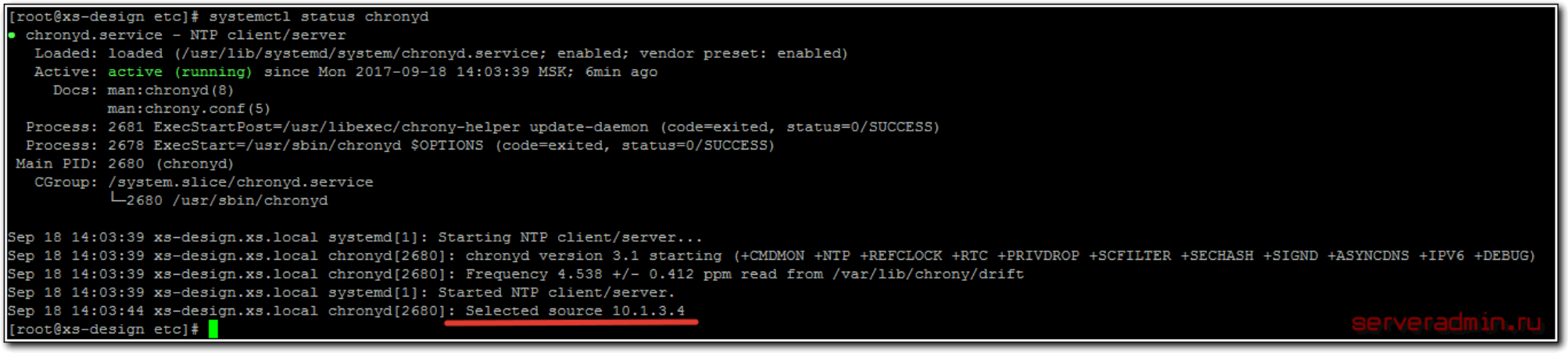
Добавляем в конфиг */etc/chrony.conf* адрес контроллера домена. И делаем его единственным сервером для синхронизации, остальные удаляем.

```
server xs-winsrv.xs.local iburst
```

Сохраняем конфиг, запускаем chrony и добавляем в автозагрузку.

```
# systemctl start chronyd && systemctl enable chronyd
```

Проверим, что с синхронизацией.



Устанавливаем софт, который понадобится для дальнейшей работы.

```
# yum install realmd sssd sssd-libwbclient oddjob oddjob-mkhomedir adcli samba-common samba-common-tools
```

Делаем проверку перед вводом в домен.

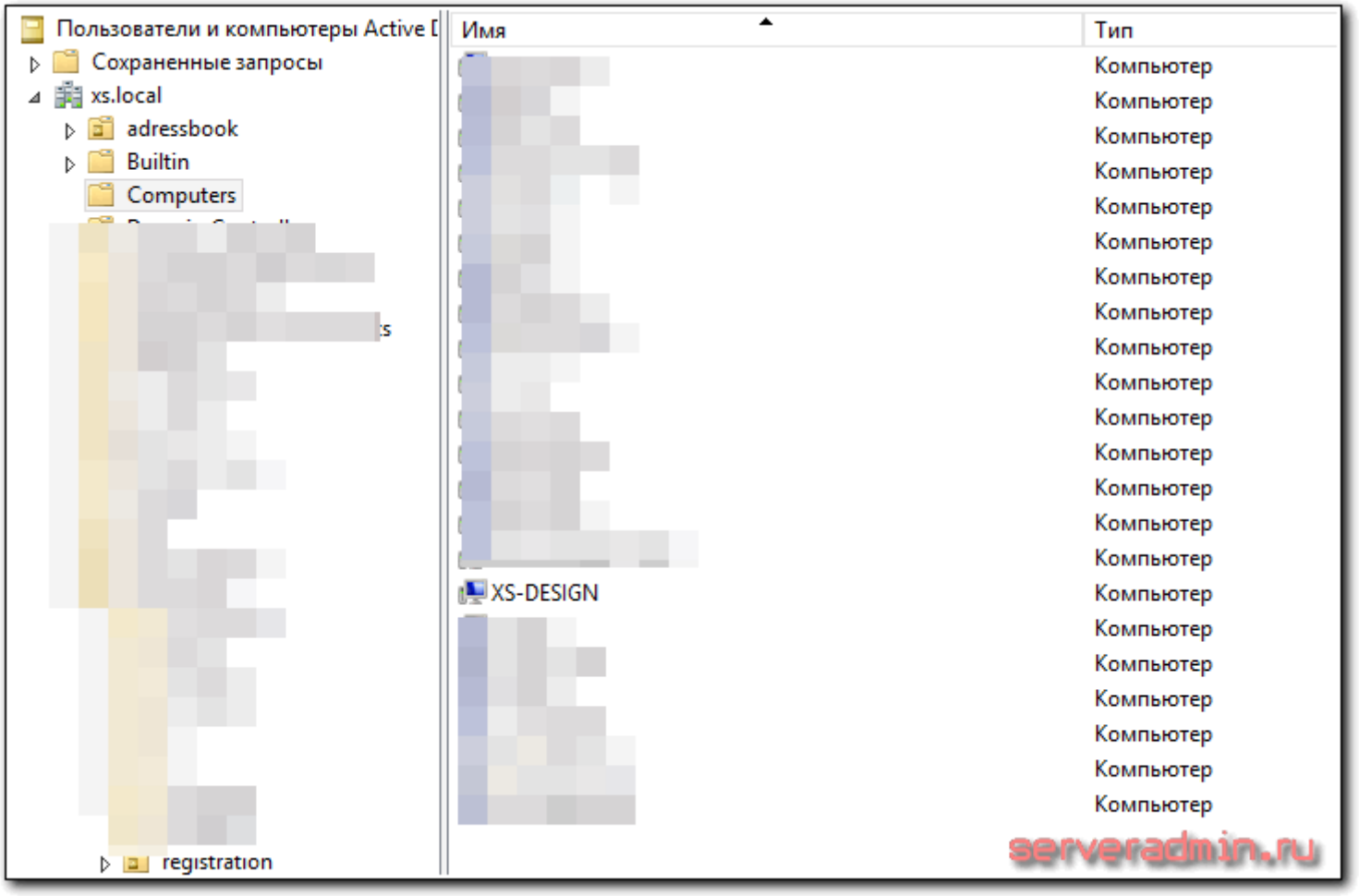
```
# realm discover XS.LOCAL
xs.local
 type: kerberos
 realm-name: XS.LOCAL
 domain-name: xs.local
 configured: no
 server-software: active-directory
 client-software: sssd
 required-package: oddjob
 required-package: oddjob-mkhomedir
 required-package: sssd
 required-package: adcli
```

```
 required-package: samba-common-tools
```

Заводим в домен.

```
# realm join -U admin51 XS.LOCAL
Password for admin51:
```

Если не получили никакой ошибки, значит все прошло нормально. Можно зайти на контроллер домена и проверить, появился ли наш linux сервер в домене.



Проверьте на самом сервере, что он нормально обращается к домену и получает информацию об учетных записях. Показываю на примере доменной учетной записи control.

```
# id control@xs.local
uid=185001305(control@xs.local) gid=185000513(пользователи домена@xs.local) groups=185000513(пользователи
домена@xs.local),185001329(gr_y@xs.local),185001651(gr_sams2@xs.local),185001327(gr_z@xs.local)
```

Еще несколько проверок.

```
# realm list
```

```
[root@xs-design samba]# realm list
xs.local
  type: kerberos
  realm-name: XS.LOCAL
  domain-name: xs.local
  configured: kerberos-member
  server-software: active-directory
  client-software: winbind
  required-package: oddjob-mkhomedir
  required-package: oddjob
  required-package: samba-winbind-clients
  required-package: samba-winbind
  required-package: samba-common-tools
  login-formats: xs\%U
  login-policy: allow-any-login
xs.local
  type: kerberos
  realm-name: XS.LOCAL
  domain-name: xs.local
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
  login-formats: %U@xs.local
  login-policy: allow-realm-logins
```



```
# adcli info xs.local
```

```
[root@xs-design samba]# adcli info xs.local
[domain]
domain-name = xs.local
domain-short = XS
domain-forest = xs.local
domain-controller = xs-wsus.xs.local
domain-controller-site = office
domain-controller-flags = gc ldap ds kdc timeserv closest writable full-secret ads-web
domain-controller-usable = yes
domain-controllers = xs-wsus.xs.local xm-winsrv.xs.local xs-winsrv.xs.local xm-wsus.xs.local
[computer]
computer-site = office
```


Сервер завели в домен. Приступаем к основному — настройке samba с интеграцией в AD.

Настройка Samba с интеграцией в AD через sssd

Устанавливаем сам файловый сервер самба.

```
# yum install samba
```

Рисуем ему примерно такой конфиг.

```
# cat /etc/samba/smb.conf
```

```
[global]
workgroup = XS
server string = Samba Server Version %v
log file = /var/log/samba/log.%m
log level =3
```

```
max log size = 500
security = ads
encrypt passwords = yes
passdb backend = tdbsam
realm = XS.LOCAL
load printers = no
cups options = raw
printcap name = /dev/null

[shara]
comment = My shared folder
path = /mnt/shara
public = no
writable = yes
guest ok = no
valid users = @"gr_it@xs.local"
```

Запускаем службу smb.service и добавляем в автозагрузку.

```
# systemctl start smb.service
# systemctl enable smb.service
```

Теперь идем проверять подключение к сетевому диску с какой-нибудь виндовой машины. Здесь меня ждало полное разочарование. Ничего не работало. Я бился над решение проблемы примерно 2 дня, но не смог победить. Перелопатил весь гугл по запросу «sssd samba», но не смог заставить работать эту связку.

Через поиск нашел как людей, которые бились над решением проблемы с теми же ошибками, что и у меня, так и тех у кого все работало нормально. Я проверил все гайды и конфиги, где люди говорили, что такая связка работает, но у меня она все равно не работала. Видел сообщения людей, которые так же как я, не смогли победить ошибки. Думаю, проблема кроется в различных версиях софта.

Мне стало жаль тратить время на поиски готового решения с sssd, хотя мне очень хотелось получить рабочий вариант, так как с winbind достаточно часто возникают проблемы. Я надеялся от них избавиться переходом на sssd, но не получилось. Статью не стал переделывать, сохранив то, что уже настроил.

Может быть у вас заработает.

Попутно узнал, что sssd не поддерживает NTLM авторизацию, только kerberos. Я не знаю, по какой причине, но у меня самба, судя по логам, упорно пыталась авторизовать пользователя по ntlm. В итоге, я прекратил попытки и вернулся к старому проверенному варианту с winbind. Далее расскажу, как настроить файловый сервер samba для работы в домене windows с помощью winbind.

Вводим CentOS 7 в домен с помощью winbind

Если у вас виртуальная машина, проще установить ее с нуля. Если не хочется по какой-то причине, можно просто удалить все установленные ранее пакеты через команду yum remove. Я поступил именно так.

Устанавливаем недостающие пакеты:

```
# yum install samba-winbind samba-winbind-clients samba pam_krb5 krb5-workstation chrony
```

Не забудьте о настройке синхронизации времени, которую мы делали на предыдущих шагах. Надо это проделать, если вы сразу начали настройку с данного пункта. Так же убедитесь, что все в порядке с dns, и контроллеры домена пингуются по именам.

Формируем конфиг для kerberos.

```
# authconfig --enablekrb5 --krb5kdc=xs-winsrv.xs.local --krb5adminserver=xs-winsrv.xs.local --krb5realm=XS-WINSRV.XS.LOCAL --enablewinbind --enablewinbindauth --smbsecurity=ads --smbrealm=XS.LOCAL --smbservers=xs-winsrv.xs.local --smbworkgroup=XS --winbindtemplatehomedir=/home/%U --winbindtemplateshell=/bin/bash --enablemkhomedir --enablewinbindusedefaultdomain --update
```

Для удобства дублирую таблицу с информацией, чтобы не пришлось скролить страницу вверх.

Информационная таблица

xs.local	название домена
10.1.3.4	ip адрес контроллера домена
xs-winsrv.xs.local	полное имя контроллера домена
xs-design	имя сервера centos, который вводим в домен

admin51 учетная запись администратора домена

Вывод после работы команды у меня такой:

```
Job for winbind.service failed because the control process exited with error code. See "systemctl status winbind.service"
and "journalctl -xe" for details.
```

Это не страшно, продолжаем настройку. Заводим сервер с CentOS в домен:

```
# net ads join -U admin51
```

На выходе получил:

```
Enter admin51's password:
Using short domain name -- XS
Joined 'XS-DESIGN' to dns domain 'xs.local'
No DNS domain configured for xs-design. Unable to perform DNS Update.
DNS update failed: NT_STATUS_INVALID_PARAMETER
```

В принципе, ничего страшного. Нам придется самим создать A запись на DNS сервере. Я не понимаю, почему иногда она не создается автоматически. Во время написания статьи, я использовал один сервер, у него не было этой ошибки при вводе в домен. Когда проверял статью на втором сервере, получил эту ошибку. Проверяем на контроллере домена в списке компьютеров наш сервер и создаем руками A запись, соответствующую имени сервера и его IP адресу.

Теперь рисуем конфиг для самбы примерно такой.

```
# mcedit /etc/samba/smb.conf
```

```
[global]
   workgroup = XS
   password server = xs-winsrv.xs.local
```

```
   realm = XS.LOCAL
   security = ads
   idmap config * : range = 16777216-33554431
   template homedir = /home/%U
   template shell = /bin/bash
   kerberos method = secrets only
   winbind use default domain = true
   winbind offline logon = false

   passdb backend = tdbsam

   load printers = no
   show add printer wizard = no
   printcap name = /dev/null
   disable spoolss = yes

   domain master = no
   local master = no
   preferred master = no
   os level = 1

   log level = 3
   log file = /var/log/samba/log.%m

[shara]
   path = /mnt/shara
   writeable = yes
   browsable = yes
   valid users = "@XS\Пользователи домена"
   admin users = "@XS\Администраторы домена"
   create mask = 0600
   directory mask = 0700
```

У меня русский язык на контроллере домена, поэтому и имена групп на русском. Проблем с этим не возникает. Не забудьте создать директорию */mnt/shara*.

Запускаем samba и winbind и добавляем в автозагрузку.

```
# systemctl start winbind
# systemctl start smb.service
# systemctl enable winbind
# systemctl enable smb.service
```

Выполняем ряд проверок, чтобы убедиться, что все в порядке, winbind работает и samba будет получать актуальную информацию о пользователях и группах домена.

```
# wbinfo -t
checking the trust secret for domain XS via RPC calls succeeded
```

```
# wbinfo -u
# wbinfo -g
```

Последние две команды должны вывести список всех пользователей и групп домена.

Проверим теперь авторизацию в домене.

```
# wbinfo -a XS\\control%'pass'
plaintext password authentication succeeded
challenge/response password authentication succeeded
```

В данном случае control — имя пользователя домена, pass — его пароль. Успешная проверка выглядит так, как у меня. В завершении проверок посмотрим, корректно ли система сопоставляет доменные учетные записи локальным.

```
# id control
uid=16777216(control) gid=16777220(пользователи домена) groups=16777220(пользователи
```

```
домена),16777221(gr_z),16777222(gr_sams2),16777223(gr_y),16777217(BUILTIN\users)
```

Все в порядке. Теперь все готово для корректной работы файлового сервера на основе Samba с доменными учетными записями. В завершении настроек, сделаем администратора домена владельцем нашей шары.

```
# chown admin51:'пользователи домена' /mnt/shara
```

Проверяем, что получилось.

```
# ll /mnt
total 0
drwxr-xr-x 2 admin51 пользователи домена 6 Sep 27 17:15 shara
```

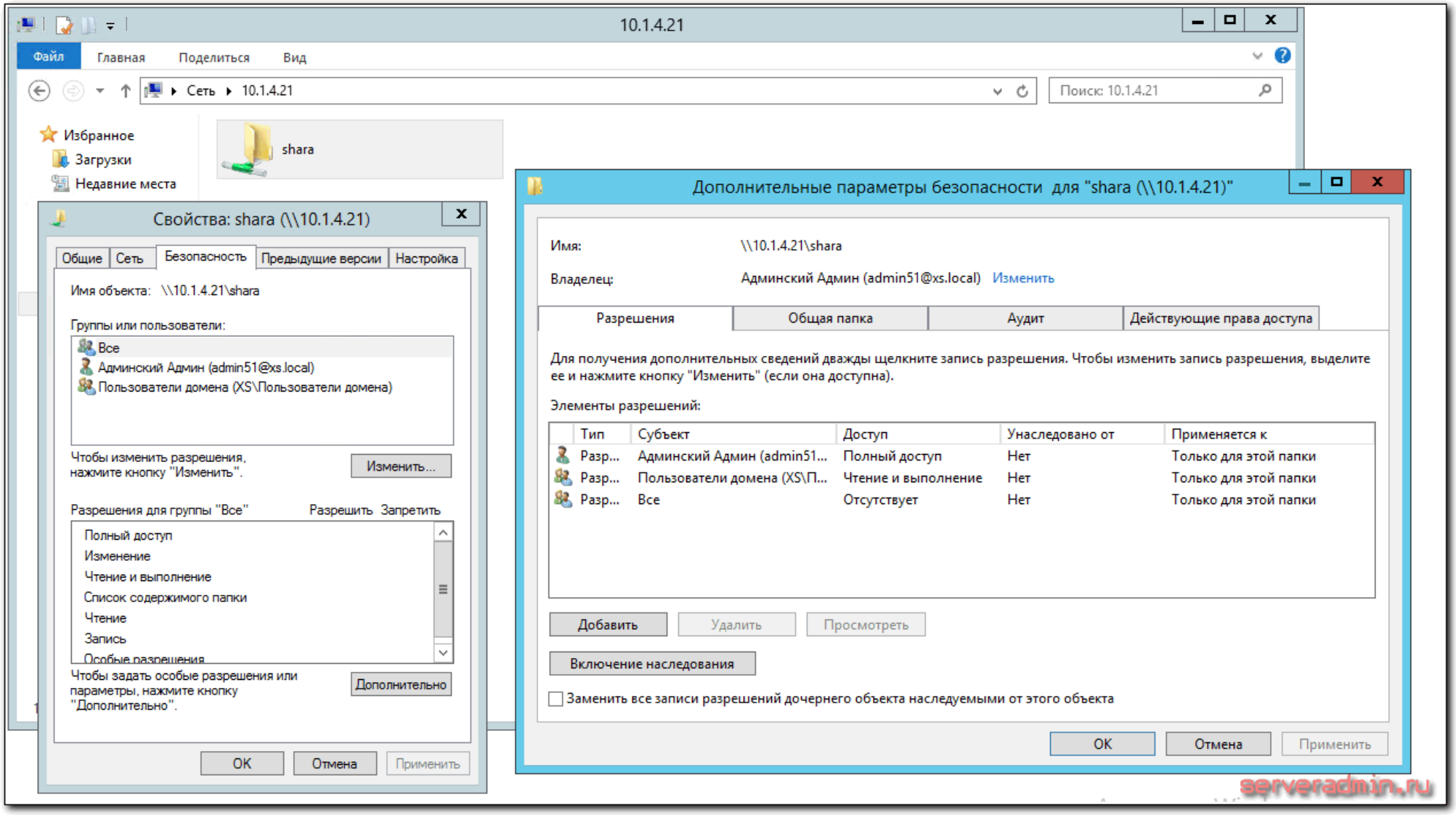
Уберем доступ на чтение у всех остальных, оставим полные права для пользователя admin51 и на чтение у пользователей домена.

```
# chmod 0750 /mnt/shara
```

Идем на любую виндовую машину и пробуем зайти на шару по адресу \\ip-адрес-сервера. Попадаем на нашу шару.

> Если не получилось зайти, проверьте настройки iptables. На время отладки можно их отключить. Так же убедитесь, что у вас запущена служба smb.service.

Смотрим расширенные параметры безопасности:


10.1.4.21
Файл
Главная
Поделиться
Вид
Сеть ▸ 10.1.4.21
Поиск: 10.1.4.21
Избранное
Загрузки
Недавние места
shara
Свойства: shara (\\10.1.4.21)
Общие
Сеть
Безопасность
Предыдущие версии
Настройка
Имя объекта: \\10.1.4.21\shara
Группы или пользователи:
Все
Администратор (admin51@xs.local)
Пользователи домена (XS\Пользователи домена)
Чтобы изменить разрешения, нажмите кнопку "Изменить".
Изменить...
Разрешения для группы "Все"
Разрешить
Запретить
Полный доступ
Изменение
Чтение и выполнение
Список содержимого папки
Чтение
Запись
Особые разрешения
Чтобы задать особые разрешения или параметры, нажмите кнопку "Дополнительно".
Дополнительно
OK
Отмена
Применить
Дополнительные параметры безопасности для "shara (\\10.1.4.21)"
Имя:
\\10.1.4.21\shara
Владелец:
Администратор (admin51@xs.local)
Изменить
Разрешения
Общая папка
Аудит
Действующие права доступа
Для получения дополнительных сведений дважды щелкните запись разрешения. Чтобы изменить запись разрешения, выделите ее и нажмите кнопку "Изменить" (если она доступна).
Элементы разрешений:
Тип
Субъект
Доступ
Унаследовано от
Применяется к
Разр...
Администратор (admin51...
Полный доступ
Нет
Только для этой папки
Разр...
Пользователи домена (XS\П...
Чтение и выполнение
Нет
Только для этой папки
Разр...
Все
Отсутствует
Нет
Только для этой папки
Добавить
Удалить
Просмотреть
Включение наследования
Заменить все записи разрешений дочернего объекта наследуемыми от этого объекта
OK
Отмена
Применить
serveradmin.ru

Получилось то, что хотели. Управлять правами доступа можно через **windows acl** с любой машины windows, где учетная запись пользователя домена будет обладать необходимыми правами. Если по какой-то причине это не получится (а я с такими ситуациями сталкивался достаточно часто), на помощь придут консольные утилиты **getfacl** для проверки прав и **setfacl** для изменения прав. Документация по этим командам есть в сети и легко ищется. Я рекомендую всегда использовать эти команды, когда вы выполняете изменение прав по большому дереву каталогов. Через консоль выставление прав будет выполнено раз в 5-10 быстрее, чем через windows acl. На больших файловых архивах разница может быть в десятки минут или даже часы.

Настройка прав доступа на файлы в Samba

Сделаю небольшое пояснение по правам доступа в файловом сервере samba. Вопрос этот сложный и объемный. Ему можно посвятить и отдельную статью. Но для полноты картины по настройке самбы, расскажу самое основное.

Как я уже ранее сказал, изменять права доступа к каталогам на файловом сервере можно с помощью команды setfacl. Давайте сейчас посмотрим на права доступа, которые установлены:

```
# getfacl /mnt/samba

# file: mnt/shara
# owner: admin51
# group: пользователи\040домена
user::rwx
group::r-x
other::---
```

С такими правами что-то создавать в папке сможет только пользователь admin51, а пользователи домена смогут только просматривать файлы и каталоги. Сделаем более прикладной вариант. Добавим права доступа на чтение и запись еще одной доменной группе — gr_it.

```
# setfacl -m g:gr_it:rwx /mnt/shara
```

Обращаю внимание, что иногда при копировании команд setfacl они не отрабатывают, выдавая не очень понятную ошибку:

```
setfacl: Option -m: Invalid argument near character 1
```

Наберите команду с клавиатуры, либо просто удалите и наберите снова ключ -m, он почему-то при копировании часто дает эту ошибку.

Смотрим, что получилось:

```
# getfacl /mnt/shara

# file: mnt/shara
# owner: admin51
# group: пользователи\040домена
user::rwx
group::r-x
group:gr_it:rwx
mask::rwx
other::---
```

То, что надо. Теперь пользователи группы gr_it имеют полные права на шару. Создадим одним таким пользователем папку *test1* на нашей шаре и посмотрим, какие права она получит.

```
# getfacl /mnt/shara/test1

# file: mnt/shara/test1
# owner: user1
# group: пользователи\040домена
user::rwx
group::---
other::---
```

Права на папку имеет только ее создатель и больше никто. Для того, чтобы наследовались права с вышестоящего каталога, необходимо на этот вышестоящий каталог добавить дефолтные права доступа. Примерно вот так.

```
# setfacl -m d:g:gr_it:rwx,d:g:'пользователи домена':rx /mnt/shara
```

Смотрим, что получилось:

```
# getfacl /mnt/shara

# file: mnt/shara
# owner: admin51
# group: пользователи\040домена
user::rwx
group::r-x
group:gr_it:rwx
mask::rwx
other::---
default:user::rwx
default:group::r-x
default:group:пользователи\040домена:r-x
default:group:gr_it:rwx
default:mask::rwx
default:other::---
```

Создадим теперь тем же пользователем еще одну папку *test2* и проверим ее права.

```
# getfacl /mnt/shara/test2

# file: mnt/shara/test2
# owner: user
# group: пользователи\040домена
user::rwx
group::---
group:пользователи\040домена:r-x
group:gr_it:rwx
mask::rwx
other::---
default:user::rwx
default:group::r-x
```

```
default:group:пользователи\040домена:r-x
default:group:gr_it:rwx
default:mask::rwx
default:other::---
```

Применилось наследование с вышестоящих папок. Не забывайте про дефолтные права и учитывайте их при настройке прав доступа на файловом сервере.

Для удобной и корректной работы с правами доступа я обычно для крупных, корневых директорий выставляю права аккуратно через setfacl в консоли. Какие-то мелкие изменения по пользователям и группам в более низших иерархиях директорий делаю через windows acl с какой-нибудь виндовой машины.

Еще важно знать одну особенность выставления прав доступа в linux. В моей практике часто требуется дать какому-нибудь пользователю доступ в одну директорию, которая располагается там, где у пользователя нет вообще никаких прав. В windows эта проблема решается просто — даются права на конкретную папку, а пользователю кладется ярлык на эту папку. В итоге он имеет доступ к нужной директории и больше никуда.

В linux так сделать не получится. Для того, чтобы дать таким образом доступ на отдельную директорию пользователю, необходимо, чтобы по всем вышестоящим директориям у него были права на исполнение, то есть **X**. Их придется выставлять вручную по всем вышестоящим папкам. Результат будет такой же, как и в винде — пользователь получит доступ на чтение только в указанную папку, но для этого придется выполнить больше действий. Если не знаешь этот нюанс, можно потратить много времени, прежде чем поймешь, в чем проблема.

Заключение

Скажу откровенно — мне не нравится, как работают файловые сервера samba с интеграцией в виндовом домене. Но настраивать их приходится часто, так как востребованный функционал. Востребован в первую очередь потому, что не требует вообще никаких денег за лицензии, и работает на минимальной конфигурации железа. Вот список типичных проблем при работе самбы в домене:

- Иногда через windows acl права перестают выставляться, возникают неинформативные ошибки, по которым невозможно понять, что не так.
- Я достаточно регулярно наблюдаю ситуацию, когда слетают соответствия доменных учеток линуксовым UID. В итоге права доступа превращаются в ничего не значащий набор цифр и перестают работать.
- При переносе данных с одного сервера на другой трудно сохранить права доступа. Можно поступить вот так для копирования прав доступа, либо как-то заморочиться, чтобы на всех серверах у вас были одинаковые UID доменных учетных записей. Я не разбирал этот вопрос подробно.

Если у вас есть возможность настроить файловый сервер на windows, либо обойтись линуксом без домена, то сделайте так. Существенно упростите настройку и дальнейшую эксплуатацию. Данную статью еще можно дополнить некоторыми моментами, которые я рассказал ранее, а что не рассказал,

постараюсь раскрыть позже и добавить сюда ссылки на статьи:

1. Подробное логирование всех действий с файлами на сервере.
2. Настройка корзины для сетевых дисков samba.
3. Бэкап файлового сервера.
4. Мониторинг за размером файловой шары.

Буду рад любым полезным замечаниям, исправлениям, советам по настройке файлового сервера samba. Я потратил значительное время, чтобы поделиться своими знаниями и опытом с остальными. Надеюсь, кто-то поделится чем-то полезным со мной. В том числе ради этого я и пишу статьи. Они расширяют мой кругозор и закрепляют полученные знания.