Ввод компьютера в домен Windows

Содержание

Введение

Зачастую возникает необходимость ввести Linux-машину в существующий домен Windows. Например, чтобы сделать файловый сервер с помощью Samba. Сделать это очень просто, для этого вам понадобятся клиент Kerberos, Samba и Winbind.

Перед установкой желательно обновиться:

```
sudo aptitude update
sudo aptitude upgrade
```

Установить всё это добро можно командой:

```
sudo aptitude install krb5-user samba winbind
```

Либо, если вы используете Ubuntu Desktop, те же пакеты можно поставить через менеджер пакетов Synaptic.

Далее вам потребуется настроить все вышеперечисленные инструменты для работы с вашим доменом. Допустим, вы хотите войти в домен **DOMAIN.COM**, доменконтроллером которого является сервер **dc.domain.com** с IP адресом **192.168.0.1**. Этот же сервер является и первичным DNS сервером домена. Кроме того допустим у вас есть второй доменконтроллер[1)], он же DNS - **dc2.domain.com** с IP **192.168.0.2**. Ваш же компьютер будет называться **smbsrv01**.

Настройка DNS

Для начала необходимо изменить настройки DNS на вашей машине, прописав в качестве DNS сервера доменконтроллер[2)] и в качестве домена поиска - нужный домен.

Если у вас статический IP-адрес, то в Ubuntu Desktop это можно сделать через Network Manager, в Ubuntu Server необходимо изменить содержимое файла `/etc/resolv.conf` на примерно такое:

```
domain domain.com
search domain.com
nameserver 192.168.0.1
```

```
nameserver 192.168.0.2
```

В современных дистрибутивах файл resolv.conf создается автоматически и править вручную его не нужно. Для получение нужного результата нужно добавить необходимые изменения в файл: `/etc/resolvconf/resolv.conf.d/head` Данные которые будут добавлены в него, будут автоматически вставлены в файл `/etc/resolv.conf`

Если IP-адрес динамический и присваивается DHCP сервером то после перезагрузки resolv.conf может формироваться «неправильный» resolv.conf' , например присутствует только один nameserver 192.168.0.1 и не указаны domain и search. Нужно отредактировать `/etc/dhcp/dhclient.conf`. Чтобы появились записи domain и search нужно убрать комментарий перед строкой supersede domain-name, и вписать свой домен:

```
supersede domain-name "domain.com";
```

Чтобы добавить еще один nameserver нужно убрать комментарий перед prepend domain-name-servers и указать ip сервера:

```
prepend domain-name-servers 192.168.0.2;
```

Для применения изменений остается перезапустить службу:

```
/etc/init.d/networking restart
```

Теперь убедитесь, что вы задали нужное имя компьютера в файле `/etc/hostname`:

```
smbsrv01
```

Кроме того необходимо отредактировать файл `/etc/hosts` так, чтобы в нём была запись с полным доменным именем компьютера и *обязательно* коротким именем хоста, ссылающаяся на один из внутренних IP:

```
# Имена этого компьютера
127.0.0.1       localhost
127.0.1.1       smbsrv01.domain.com    smbsrv01
```

Сразу нужно проверить что нормально пингуется наш контроллер домена, по короткому и полному имени, чтобы в будушем не получать ошибки что контроллер домена не найден:

```
ping dc
ping dc.domain.com
```

Не обязательно, но если вы что-то поменяете - перезагрузите компьютер для применения изменений.

Настройка синхронизации времени

Далее необходимо настроить синхронизацию времени с доменконтроллером. Если разница будет более 5 минут мы не сможем получить лист от Kerberos. Для единовременной синхронизации можно воспользоваться командой:

```
sudo net time set dc
```

Если в сети существует сервер точного времени, то можно воспользоваться им или любым публичным:

```
ntpdate ntp.mobatime.ru
```

Автоматическая же синхронизация настраивается с помощью `ntpd`, это демон будет периодически выполнять синхронизацию. Для начала его необходимо установить:

```
sudo aptitude install ntp
```

Теперь исправьте файл `/etc/ntp.conf`, добавив в него информацию о вашем сервере времени:

```
# You do need to talk to an NTP server or two (or three).
server dc.domain.com
```

После чего перезапустите демон `ntpd`:

```
sudo /etc/init.d/ntp restart
```

Теперь пора настраивать непосредственно взаимодействие с доменом.

Настройка авторизации через Kerberos

Начнём с настройки авторизации в домене через протокол Kerberos. Вам потребуется изменить файл `/etc/krb5.conf`. В общем случае он выглядит так:

```
[libdefaults]
        default_realm = DOMAIN.COM
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true
        v4_instance_resolve = false
        v4_name_convert = {
                host = {
                        rcmd = host
                        ftp = ftp
                }
                plain = {
                        something = something-else
                }
        }
        fcc-mit-ticketflags = true

[realms]
        DOMAIN.COM = {
                kdc = dc
                kdc = dc2
                admin_server = dc
                default_domain = DOMAIN.COM
        }

[domain_realm]
        .domain.com = DOMAIN.COM
        domain.com = DOMAIN.COM
[login]
        krb4_convert = false
        krb4_get_tickets = false
```

Вам, конечно, нужно изменить `domain.com` на ваш домен и `dc` и `dc2` на ваши доменконтроллеры. Кстати, возможно вам понадобится написать полные имена доменконтроллеров `dc.domain.com` и `dc2.domain.com`. Поскольку у меня прописан домен поиска в DNS, то мне это делать не нужно.

Обратите особое внимание на регистр написания имени домена - везде, где домен написан в верхнем регистре, его обязательно нужно писать именно в верхнем регистре. Иначе волшебным образом ничего может не заработать.

Это не все возможные опции настройки Kerberos, только основные. Однако их обычно достаточно.

Теперь настало время проверить, что мы можем авторизоваться в домене. Для этого выполните команду

```
kinit username@DOMAIN.COM
```

Вместо username естественно стоит вписать имя существующего пользователя домена.

Имя домена необходимо писать заглавными буквами!

Если вы не получили никаких ошибок - значит вы настроили всё верно и домен отдаёт вам билет Kerberos. Кстати, некоторые распространённые ошибки перечислены чуть ниже.

Убедиться в том, что билет получен, можно выполнив команду

```
klist
```

Удалить все билеты (они вам вообще говоря не нужны) можно командой

```
kdestroy
```

Итак, будем считать, что авторизацию вы настроили, пора настроить непосредственно вход в домен, об этом после списка распространённых ошибок `kinit`.

Распространённые ошибки kinit

```
kinit(v5): Clock skew too great while getting initial credentials
```

Это значит, что у вашего компьютера не синхронизировано время с доменконтроллером (см. выше).

```
kinit(v5): Preauthentication failed while getting initial credentials
```

Вы ввели неверный пароль.

```
kinit(v5): KDC reply did not match expectations while getting initial credentials
```

Самая странная ошибка. Убедитесь, что имя realm в `krb5.conf`, а так же домен в команде `kinit` введены большими буквами:

```
DOMAIN.COM = {
# ...
kinit username@DOMAIN.COM
kinit(v5): Client not found in Kerberos database while getting initial credentials
```

Указанного пользователя не существует в домене.

Настройка Samba и вход в домен

Для того, чтобы войти в домен, необходимо прописать правильные настройки в файле `/etc/samba/smb.conf`. На данном этапе вас должны интересовать только некоторые опции из секции `[global]`. Ниже - пример части файла конфигурации Samba с комментариями по поводу значения важных параметров:

```
[global]
   # Эти две опции нужно писать именно в заглавном регистре, причём workgroup без
   # последней секции после точки, а realm - полное имя домена
```

```
   workgroup = DOMAIN
   realm = DOMAIN.COM

   # Эти две опции отвечают как раз за авторизацию через AD
   security = ADS
   encrypt passwords = true
   # Просто важные
   dns proxy = no
   socket options = TCP_NODELAY

   # Если вы не хотите, чтобы самба пыталась при случае вылезти в лидеры в домене или
рабочей группе,
   # или даже стать доменконтроллером, то всегда прописывайте эти пять опций именно в
таком виде
   domain master = no
   local master = no
   preferred master = no
   os level = 0
   domain logons = no

   # Отключить поддержку принтеров
   load printers = no
   show add printer wizard = no
   printcap name = /dev/null
   disable spoolss = yes
```

После того, как вы отредактируете `smb.conf` выполните команду

```
testparm
```

Она проверит вашу конфигурацию на ошибки и выдаст суммарную сводку о нём:

```
# testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER
Press enter to see a dump of your service definitions
```

Как видно мы задали правильные параметры для того, чтобы наш компьютер стал членом домена. Теперь пора попытаться непосредственно войти в домен. Для этого введите команду:

```
net ads join -U username -D DOMAIN
```

И в случае успеха вы увидите что-то похожее на:

```
# net ads join -U username -D DOMAIN
Enter username's password:
Using short domain name -- DOMAIN
Joined 'SMBSRV01' to realm 'domain.com'
```

Используемые параметры команды net

`-U username%password`: Обязательный параметр, вместо `username` необходимо подставить имя пользователя с правами администратора домена, и указать пароль.

`-D DOMAIN`: `DOMAIN` - собственно сам домен, домен можно и не указывать, но лучше всё же это всегда делать - хуже не будет.

`-S win_domain_controller`: `win_domain_controller`, можно не указывать, но бывают случаи когда автоматически сервер не находит контроллер домена.

`createcomputer=«OU/OU/…»` : В AD часто используется OU (Organizational Unit), есть в корне домена OU = Office, в нем OU = Cabinet, чтобы сразу добавить в нужный можно указать так: sudo net ads join -U username createcomputer=«Office/Cabinet».

Если больше никаких сообщений нет - значит всё хорошо. Попробуйте попинговать свой компьютер по имени с другого члена домена, чтобы убедиться, что в домене всё прописалось так, как надо.

Так же можно набрать команду:

```
net ads testjoin
```

Если все хорошо, можно увидеть:

```
#net ads testjoin
Join is OK
```

Но иногда после сообщения о присоединении к домену выдаётся ошибка наподобие[3)]:

```
DNS update failed!
```

Это не очень хорошо, и в этом случае рекомендуется ещё раз прочитать раздел про настройку DNS чуть выше и понять, что же вы сделали не так. После этого нужно удалить компьютер из домена и попытаться ввести его заново. Если вы твердо уверены, что всё настроили верно, а DNS всё равно не обновляется, то можно внести вручную запись для вашего компьютера на ваш DNS сервер и всё будет работать. Конечно, если нет никаких других ошибок, и вы успешно вошли в домен. Однако лучше всё же разберитесь, почему DNS не обновляется автоматически. Это может быть связано не только с вашим компьютером, но и с некорректной настройкой AD.

Прежде чем выяснять, почему же не обновляется DNS, не забудьте перезагрузить компьютер после введения в домен! Вполне возможно, что это решит проблему.

Если всё прошло без ошибок, то поздравляем, вы успешно вошли в домен! Можете заглянуть в AD и убедиться в этом. Кроме того хорошо бы проверить, что вы можете видеть ресурсы в домене. Для этого установите `smbclient`:

```
sudo aptitude install smbclient
```

Теперь можно просматривать ресурсы компьютеров домена. Но для этого нужно иметь билет kerberos, т.е. если мы их удалили, то получаем опять через kinit (см. выше). Посмотрим какие ресурсы предоставлены в сеть компьютером `workstation`:

```
smbclient -k -L workstation
```

Вы должны увидеть список общих ресурсов на этом компьютере.

Настройка Winbind

Если вам необходимо как-либо работать с пользователями домена, например, настраивать SMB-шары с разграничением доступа, то вам понадобится кроме самой Samba ещё и Winbind - специальный демон, служащий для связи локальной системы управления пользователями и группами Linux с сервером Active Directory. Проще говоря Winbind нужен, если вы хотите видеть пользователей домена на своём компьютере с Ubuntu.

Winbind позволяет спроецировать всех пользователей и все группы AD в вашу Linux систему, присвоив им ID из заданного диапазона. Таким образом вы сможете назначать пользователей домена

владельцами папок и файлов на вашем компьютере и выполнять любые другие операции, завязанные на пользователей и группы.

Для настройки Winbind используется всё тот же файл `/etc/samba/smb.conf`. Добавьте в секцию `[global]` следующие строки:

```
   # Опции сопоставления доменных пользователей и виртуальных пользователей в системе
через Winbind.
   # Диапазоны идентификаторов для виртуальных пользователей и групп.
   idmap uid = 10000 - 40000
   idmap gid = 10000 - 40000
   # Эти опции не стоит выключать.
   winbind enum groups = yes
   winbind enum users = yes
   # Использовать домен по умолчанию для имён пользователей. Без этой опции имена
пользователей и групп
   # будут использоваться с доменом, т.е. вместо username - DOMAIN\username.
   # Возможно именно это вам и нужно, однако обычно проще этот параметр включить.
   winbind use default domain = yes
   # Если вы хотите разрещить использовать командную строку для пользователей домена,
то
   # добавьте следующую строку, иначе в качестве shell'а будет вызываться /bin/false
   template shell = /bin/bash
   # Для автоматического обновления билета Kerberos модулем pam_winbind.so нужно
добавить строчку
   winbind refresh tickets = yes
```

Параметры :

idmap uid = 10000 - 40000

idmap gid = 10000 - 40000

в новых версиях Samba уже устарели и при проверке конфига самбы с помощью testparm будет выдваться предупреждение:

WARNING: The «idmap uid» option is deprecated

WARNING: The «idmap gid» option is deprecated

Чтобы убрать предупреждения нужно заменить эти строки на новые:

idmap config * : range = 10000-20000

idmap config * : backend = tdb

Теперь перезапустите демон Winbind и Samba в следующем порядке:

```
sudo /etc/init.d/winbind stop
sudo smbd restart
sudo /etc/init.d/winbind start
```

Запускаем

```
sudo testparm
```

Смотрим есть ли ошибки или предупреждения, если появится:

«rlimit_max: rlimit_max (1024) below minimum Windows limit (16384)»

Без перезагрузки можно устранить так:

```
ulimit -n 16384
```

Для сохранения после перезагрузки отредактировать файл /etc/security/limits.conf

```
# Добавить в конец файла строки:
*               -    nofile            16384
root            -    nofile            16384
```

После перезапуска проверьте, что Winbind установил доверительные отношения с AD командой:

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

А так же, что Winbind увидел пользователей и группы из AD командами[4)]:

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

Эти две команды должны выдать список пользователей и групп из домена соответственно. Либо с префиксом `DOMAIN\`, либо без него - в зависимости от того, какое значение вы указали параметру «winbind use default domain» в `smb.conf`.

Итак, Winbind работает, однако в систему он ещё не интегрирован.

Добавление Winbind в качестве источника пользователей и групп

Для того, чтобы ваша Ubuntu прозрачно работала с пользователями домена, в частности, чтобы вы могли назначать пользователей домена владельцами папок и файлов, необходимо указать Ubuntu использовать Winbind как дополнительный источник информации о пользователях и группах.

Для этого измените две строчки в файле `/etc/nsswitch.conf`:

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

добавив к ним в конец `winbind`:

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

Теперь проверьте, что Ubuntu запрашивает у Winbind информацию о пользователях и группах, выполнив

```
getent passwd
getent group
```

Первая команда должна вам вернуть всё содержимое вашего файла `/etc/passwd`, то есть ваших локальных пользователей, плюс пользователей домена с ID из заданного вами в `smb.conf` диапазона. Вторая должна сделать тоже самое для групп.

Теперь вы можете взять любого пользователя домена и сделать его, например, владельцем какого-нибудь файла.

Авторизация в Ubuntu через пользователей домена

Несмотря на то, что все пользователи домена фактически стали полноценными пользователями системы (в чём можно убедиться, выполнив последние две команды из предыдущего раздела), зайти ни под кем из них в систему всё ещё нельзя. Для включения возможности авторизации пользователей домена на компьютере с Ubuntu необходимо настроить PAM на работу с Winbind.

Он-лайн авторизация

Для **Ubuntu 10.04 и выше** добавьте всего одну строку в файле `/etc/pam.d/common-session`, т.к. PAM и так неплохо справляется с авторизацией:

```
session  optional  pam_mkhomedir.so skel=/etc/skel/ umask=0077
```

Для **Ubuntu 9.10 и ниже** придется редактировать несколько файлов (но никто не запрещает использовать этот способ и в 10.04 - он тоже работает):

Последовательность строк в файлах имеет значение!

```
/etc/pam.d/common-auth

auth        required      pam_env.so
auth        sufficient    pam_unix.so likeauth nullok try_first_pass
auth        sufficient    pam_winbind.so use_first_pass krb5_auth krb5_ccache_type=FILE
auth        required      pam_deny.so

/etc/pam.d/common-account

account     sufficient    pam_winbind.so
account     required      pam_unix.so

/etc/pam.d/common-session

session     optional      pam_mkhomedir.so skel=/etc/skel/ umask=0077
session     optional      pam_ck_connector.so nox11
session     required      pam_limits.so
session     required      pam_env.so
session     required      pam_unix.so

/etc/pam.d/common-password

password    sufficient    pam_unix.so try_first_pass use_authtok nullok sha512 shadow
password    sufficient    pam_winbind.so
password    required      pam_deny.so
```

И, наконец, необходимо перенести запуск Winbind при загрузке системы после всех остальных служб (по умолчанию он запускается с индексом 20). Для этого в терминале выполните следующую команду:

```
sudo bash -c "for i in 2 3 4 5; do mv /etc/rc$i.d/S20winbind /etc/rc$i.d/S99winbind;
done"
```

Что эквивалентно запуску для каждого уровня (в примере - 4) команды:

```
mv /etc/rc4.d/S20winbind /etc/rc4.d/S99winbind
```

В некоторых случаях winbind может иметь иной уровень запуска (например, S02winbind). Поэтому сначала проверьте имена файлов, вполнив команду «ls /etc/rc{2,3,4,5}.d/ | grep winbind» (без кавычек).

Готово, все настройки завершены. Перезагружайтесь и пытайтесь войти с учетной записью пользователя домена.

Офф-лайн авторизация

Часто возникает ситуация, когда домен-контроллер недоступен по различным причинам — профилактика, отключение света или вы принесли ноутбук домой и хотите поработать. В этом случае для Winbind можно настроить кэширование учетных записей пользователей домена. Для этого необходимо сделать следующее. Добавьте в секцию `[global]` файла `/etc/samba/smb.conf` следующие строки:

```
[global]
   # Возможность оффлайн-авторизации при недоступности доменконтроллера
   winbind offline logon = yes
   # Период кэширования учетных записей, по умолчанию равен 300 секунд
   winbind cache time = 300
   # Необязательная настройка, но избавляет от нудных пауз, указываем контроллер домена
dc,
   # можно указать и ip, но это является плохим тоном
   password server = dc
```

Обычно этого достаточно. Если же возникают ошибки, то необходимо создать файл `/etc/security/pam_winbind.conf` со следующим содержанием[5)]:

Внимание! При использовании советов ниже может возникать совершенно случайная ошибка «Сбой аутентификации»! Поэтому все что Вы делаете, Вы делаете на свой страх и риск!

```
#
# pam_winbind configuration file
#
# /etc/security/pam_winbind.conf
#
[global]
  # turn on debugging
  debug = no
  # request a cached login if possible
  # (needs "winbind offline logon = yes" in smb.conf)
  cached_login = yes
  # authenticate using kerberos
  krb5_auth = yes
  # when using kerberos, request a "FILE" krb5 credential cache type
  # (leave empty to just do krb5 authentication but not have a ticket
  # afterwards)
  krb5_ccache_type = FILE
  # make successful authentication dependend on membership of one SID
  # (can also take a name)
  ;require_membership_of =
  silent = yes
```

Файл `/etc/pam.d/gnome-screensaver` в таком случае принимает вид:

```
auth    sufficient      pam_unix.so nullok_secure
auth    sufficient      pam_winbind.so use_first_pass
auth    required        pam_deny.so
```

А также изменяется файл `/etc/pam.d/common-auth`:

```
auth    optional        pam_group.so
auth    sufficient      pam_unix.so nullok_secure  use_first_pass
auth    sufficient      pam_winbind.so use_first_pass
auth    required        pam_deny.so
```