Сисодминиум

2014-08-24 22:40

ubuntu active directory

[Active Directory] Ubuntu в домене Windows AD

Некоторое время назад на работе достался мне для работы ноутбук HP ProBook 6460b. Ну и пришла в голову идея поставить на него вместо надоевшей Windows 7 Pro давно понравившуюся мне Ubuntu 14.04 Trusty LTS. Выбор операционной системы связан с тем, что Ubuntu я использую на домашнем ноутбуке и мне захотелось иметь такую же систему на рабочем компьютере. Потому, что постоянное переключение между ОСями дома и на работе быстро надоело мне и я решился на установку Ubuntu на рабочем ноуте.

Начну по порядку

Процесс установки Убунты на ноутбук не буду пересказывать потому, что не вижу в этом смысла из-за большого количества таких мануалов на просторах интернета. Скажу только то, что устанавливал с флешки, а образ на флешку писал на рабочем ноутбуке под Windows 7 Pro с помощью программы Rufus.
Хватит про установку, перейдем к процессу введения в домен.
При вводе в домен Windows я пользовался стандартной инструкцией по вводу в домен. В процессе ввода в домен возникали проблемы самого разного характера (в основном связанные с моей невнимательностью и легкой кривизной рук :-)). Да инструкция на русском языке есть и она довольно хороша, но я все же пользовался не только этой инструкцией, но и другими подсказками с прочих сайтов и форумов. Поэтому я решил собрать из всех одну свою.

Первое что необходимо сделать это - правильно и вполне логично! - обновиться:

```
sudo apt-get update
sudo apt-get upgrade
```

Далее нас потребуется установить клиенты `Kerberos`, `Samba` и `Winbind` для нормальной и адекватной работы в домене `Windows`. Сделать это можно одной командой:

```
sudo apt-get install krb5-user
sudo apt-get install samba
sudo apt-get install winbind
```

Лично я пробовал два варианта установки: первый - как указано выше - установка всех необходимых пакетов одной строкой, и второй - установка каждого паке в отдельности. Честно признаюсь, что меня больше устроил и больше понравился вариант отдельной установки каждого пакета. Поясню это тем, что при комплексной установке у меня начальная настройка пакета Kerberos не происходила, и я решил (точнее не решил, а мне пришлось из-за кривизны рук и невнимательности переустанавливать полностью Ubuntu и соответственно все необходимые пакеты) ставить все пакеты по отдельности в вышеуказанном порядке. Это дало свои плоды. На этапе установки пакеты `Kerberos` произошла его полная настройка где указывались все необходимые параметры для работы в домене (собственно сам домен, необходимые для авторизации `DC`, рабочие группы или зоны). Далее я поставил Самбу и Винбинд с которыми каких-либо заморочек не было. Так же я установил указанные желательными библиотеки `libpam-krb5`, `libpam-winbind` и `libnss-winbind`. Их я устанавливал одной командой, т.к. они не требуют никаких ручных настроек и просто желательно их присутствие в системе.

Для простоты и дальнейшей ясности процесса будем считать нашим доменом по умолчанию `DOMAIN.RU`, доменконтроллером которого будет `first.domain.ru` с ip-адресом `192.168.1.2`. Он же будет нашим первичным DNS сервером домена. Коме того представим в нашем домене еще один доменконтроллер `second.domain.ru` с ip-адресом `192.168.1.3`. Ну и компьютер наш будет называться `work-ubuntu`.

Настройка DNS

Для начала необходимо изменить настройки DNS на вашей машине, прописав в качестве DNS-сервера доменконтроллер 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.ru
search domain.ru
nameserver 192.168.1.2
```

```
nameserver 192.168.1.1
nameserver 127.0.1.1
search domain.ru first.domain.ru
```

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 192.168.1.1` 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.ru first.domain.ru"
```

Можно было бы добавить еще один `nameserver`, но я этого делать не стал потому, что у нас в сети компании он единственный. Для применения изменений необходимо перезапустить службу:

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

Теперь необходимо проверить файл `/etc/hostname` и убедиться в том, что мы правильно задали имя нашего ноутбука.

```
work-ubuntu
```

Кроме всего прочего необходимо отредактировать файл `/etc/hosts` так, чтобы в нем была запись с полным доменным именем и *обязательно* с коротким именем. У меня получился такой формат:

```
127.0.0.1    localhost
127.0.1.1    work-ubuntu.domain.ru    work-ubuntu
```

Сразу необходимо проверить, что наш контроллер домена пингуется нормально по короткому и по полному доменному именам:

```
ping first
ping first.domain.ru
```

Не обязательно конечно, но как говорится в инструкции “желательно” при внесении каких-либо изменений делать перезагрузку. Лично я так и делал.

Настройка синхронизации времени

Тут собственно говоря ничего сложного! Я просто единожды выполнил команду:

```
sudo net time set first
```

и забыл про это дело. Другие варианты развития я не вижу смысла освещать в статье т.к. они мне не понадобились.

Собственно переходим к самому основному: настройка авторизации через `Kerberos`

Настройка авторизации по протоколу Kerberos осуществляется простым редактированием файла `/etc/krb5.conf`. Вот примерный его вид:

```
[libdefaults]
default_realm = DOMAIN.RU

# The following krb5.conf variables are only for MIT Kerberos.
krb4_config = /etc/krb.conf
krb4_realms = /etc/krb.realms
kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true

# The following libdefaults parameters are only for Heimdal Ker
v4_instance_resolve = false
v4_name_convert = {
    host = {
```

```
        rcmd = host
        ftp = ftp
    }
    plain = {
        something = something-else
    }
}
fcc-mit-ticketflags = true

[realms]
DOMAIN.RU = {
    kdc = first.DOMAIN.RU
    admin_server = first
    default_domain = DOMAIN.RU
}

[domain_realm]
.domain.ru = DOMAIN.RU
domain.ru = DOMAIN.RU

[login]
krb4_convert = false
krb4_get_tickets = false
```

Вы естественно указываете вместо `DOMAIN.RU` и `first` свои домен и контроллер домена. Особое внимание обращаю на соблюдение регистра - все что написано в верхнем регистре пишется в верхнем регистре!

Это конечно далеко не все, что настраивается но уже сейчас возможно проверить способность авторизации в домене. Для этого достаточно выполнить команду:

```
kinit vasya@DOMAIN.RU
```

Вместо `vasya` и `DOMAIN.RU` вы так же указываете свои имя пользователя и домен. Команда так же регистрозависима! Если вы после выполнения данной команды получаете завпрос на ввод пароля от указанного пользователя и не получаете никаких ошибок, значит у вас все прекрасно. В противном случае еще раз перепроверьте все измененные вами файлы на правильность (внимательно изменяйте все ваши файлы).

Убедиться в том, что билет получен, можно с помощью команды:

```
klist
```

Будем считать, что авторизация вы настроили и билет получен. Теперь настроим вход в домен.

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 нас интересуют только некоторые параметры секции `[global]`. Вот примерный вариант файла:

```
[global]
workgroup = DOMAIN
realm = DOMAIN.RU

# 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
# или даже стать доменконтроллером, то всегда прописывайте эти
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
```

Теперь необходимо проверить внесенные изменения на правильность (точнее

себя на внимательность и руки на кривость :-)) следующей командой:

```
testparm
```

В случае правильного изменения файла `/etc/samba/smb.conf` вы увидите примерно следующее:

```
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
```

Данное сообщение известит вас о том, что вы правильно внесли все изменения и настала пора наконец-таки осуществить вход в домен. Для этого необходимо выполнить следующую команду:

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

В случае успешного входа вы увидите на экране примерно следующее:

```
Enter vasya's password:
Using short domain name -- DOMAIN
Joined 'WORK-UBUNTU' to realm 'domain.ru'
```

Я снова не стану описывать все возможные ошибки, потому что и ежу понятно, что если появились ошибки значит ты сделал что-то не так. Поэтому скажу только одно: RTFM friend!

На данном этапе вы можете установить себе `smbclient`:

```
sudo apt-get install smbclient
```

и проверить доступность ресурсов, хотя бы, на доменконтроллере:

```
smbclient -k -L first
```

Вы должны будете увидеть список доступных ресурсов на доменконтроллере

Переходим к настройке Winbin

Если вам необходимо 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 поль
# Диапазоны идентификаторов для виртуальных пользователей и гру
idmap config * : range = 5000-20000
idmap config * : backend = tdb
# Эти опции не стоит выключать.
winbind enum groups = yes winbind enum users = yes
# Использовать домен по умолчанию для имён пользователей. Без э
# будут использоваться с доменом, т.е. вместо username - DOMAIN
# Возможно именно это вам и нужно, однако обычно проще этот пар
winbind use default domain = yes
# Если вы хотите разрешить использовать командную строку для пс
# добавьте следующую строку, иначе в качестве shell'а будет выз
template shell = /bin/bash
# Для автоматического обновления билета Kerberos модулем pam_wi
winbind refresh tickets = yes
```

Строки с параметрами `idmap config` указаны с новыми параметрами не характерными для старых версий Samba, поэтому на данном этапе будьте

внимательнее. Старый формат этих строк можно посмотреть в официальной инструкции по вводу в домен.

Теперь вам необходимо перезапустить демон `Winbind` и `Samba`. Для этого соблюдая порядок команд, выполните их поочередно:

```
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)`, то 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 succeede
```

А так же, что `Winbind` увидел пользователей и группы из `AD` командами:

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

Итак, `Winbind` работает, однако в систему он еще не интегрировал.

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 конце `winbind`:

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

Так же рекомендую привести строку `hosts:` в файле `/etc/nsswitch.conf` к виду:

```
hosts:          files dns mdns4_minimal [NOTFOUND=return] mdns4
```

Теперь можно проверить, что Ubuntu запрашивает у `Winbind` информацию о пользователях и группах выполнив по очереди следующие команды:

```
getent passwd
getent group
```

После выполнения первой команды вы должны увидеть содержимое вашего файла `/etc/passwd` и пользователей вашего домена `AD` из указанного диапазона в файле `/etc/samba/smb.conf`. Вторая команда вернет все то же

самое, только для групп.

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 он-лайн авторизации я лично подредактировал парочку файлов. Первый файл, который я редактировал это `/etc/pam.d/common-session` и добавил в него всего одну строчку:

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

Вторым был файлик `/etc/lightdm/user.conf`. В него необходимо добавить строчку в самый конец файла:

```
greeter-show-manual-login=true
```

На этом собственно говоря все готово! Перезагружаемся и входим под учетной записью доменного пользователя.

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 доменконтрс
winbind offline logon = yes
```

```
# Период кэширования учетных записей, по умолчанию равен 300 се
winbind cache time = 300
# Необязательная настройка, но избавляет от нудных пауз, указыв
# 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:

```
# 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 t
# (leave empty to just do krb5 authentication but not have a ti
# afterwards)
krb5_ccache_type = FILE
# make successful authentication dependend on membership of one
# (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
```

На этом вроде бы все :-)

Вместо заключения

После всех проделанных операций наша машина на Ubuntu стала полноценным членом домена Windows и теперь с ней могу работать пользователи `AD`.

Было мягко говоря не легко. Тяжело было собрать информацию, относящуюся именно к моей `Ubuntu 14.04 Trusty LTS`.

ubuntu active directory

JTProg

RTFM!!!