

# Как подружить Linux с доменом Active Directory



**Мирослав Бусалов**

**Windows или Linux? Наверное, нет ни одного системного администратора, который не задумывался бы над этим вопросом. О плюсах и минусах операционных систем Open Source и продуктов Microsoft написаны гигабайты текстов, ожесточенные споры не утихают уже много лет. Наблюдая за этими баталиями, хочется лишь одного – гармонии.**

**П**редположим следующую ситуацию. Часть сотрудников вашей компании выполняет только рутинные операции в одном-двух бизнес-приложениях, используя браузер. И операционная система для них значения не имеет. Исходя из экономической целесообразности, нет смысла ставить на такие рабочие станции Windows.

Или другой пример – есть отдел разработчиков под UNIX, которым удобнее и комфортнее использовать на рабочей станции Linux. Как можно заметить, причины внедрения Linux-

десктопов в организации могут быть различные. При этом в вашей организации есть домен Active Directory, все пользователи имеют свои учетные записи, собственные папки на файловом сервере и разные права на свои рабочие станции. Подобные удобства всем хотелось бы сохранить и на рабочих станциях под Linux, особенно системному администратору, поскольку централизованная авторизация и хранение данных пользователей на сервере уменьшают его головную боль.

Статья представляет собой пошаговое руководство, как «подружить»

рабочие станции Linux с доменом Active Directory.

## **Начальные условия**

Домен Active Directory под управлением одного или более контроллеров домена на базе Windows Server 2003; в качестве Linux-десктопа используется Kubuntu 7.10

## **Цели**

- Обеспечить единую аутентификацию пользователей.
- Обеспечить авторизацию пользователей в домене Active Directory.

- Обеспечить прозрачную и сквозную авторизацию на ресурсах сети (SSO – Single Sign-On).
- Обеспечить хранение пользовательских данных на сервере.

Про последний пункт хотелось бы сказать следующее: в данном примере в качестве файлового сервера используется Windows-сервер. Поэтому речь идет только о хранении данных пользователей. Сохранять профиль UNIX-пользователя на сервере не представляется возможным, так как в качестве Linux-деSKTOPа используется Kubuntu 7.10 со встроенным экраным менеджером KDE. В процессе создания профиля пользователя KDE создает символичные ссылки (symlink), которые необходимы для корректной работы. Естественно, что создать symlink в файловой системе NTFS на Windows Server 2003 не получится.

### Используемые обозначения

- **domain.ru** – полное имя домена Active Directory;
- **dc.domain.ru** – полное имя контроллера домена;
- **fileserver.domain.ru** – полное имя файлового сервера.

Условно всю работу можно разделить на следующие этапы:

- Модернизация схемы Active Directory.
- Настройка атрибутов будущих UNIX-пользователей и групп.
- Настройка рабочей станции с Kubuntu.
- Настройка ресурсов сети (веб-серверов, службы ssh и т. д.) для обеспечения прозрачной и сквозной авторизации пользователей.

### Модернизация схемы Active Directory

В классической схеме AD невозможно хранить атрибуты UNIX-пользователей, такие как UID, GID, Login Shell, Home Directory. Поэтому схему необходимо расширить, добавив в нее возможность хранения нужных нам сведений. Для этого существует два варианта: первый – это бесплатный пакет Microsoft под названием Windows Services for UNIX 3.5 (SFU), второй – это использование последней версии семейства серверов 2003 – Windows

Server 2003 R2. Мы будем использовать второй вариант. Если ваши контроллеры домена и файловые серверы уже работают под релизом R2, можно смело пропустить несколько абзацев, касающихся обновления стандартного Windows Server 2003 до R2.

Windows Server 2003 R2 – версия Windows Server 2003, имеющая встроенные компоненты Windows Services for UNIX (SFU), необходимые нам при создании гетерогенной среды для хранения атрибутов UNIX-пользователей в схеме Active Directory. Релиз R2 включает в себя два важных компонента:

- Subsystem for UNIX-based Applications (SUA);
- Identity Management for UNIX (IMU).

SUA помогает UNIX-приложениям работать под Windows так, как будто они работают в Linux или UNIX. Это выходит за рамки нашей статьи, поэтому мы сфокусируем внимание на компоненте IMU, которая содержит нужные в дальнейшем службы – Administration Components, Password Synchronization, Server for NIS, их установку мы сейчас и рассмотрим.

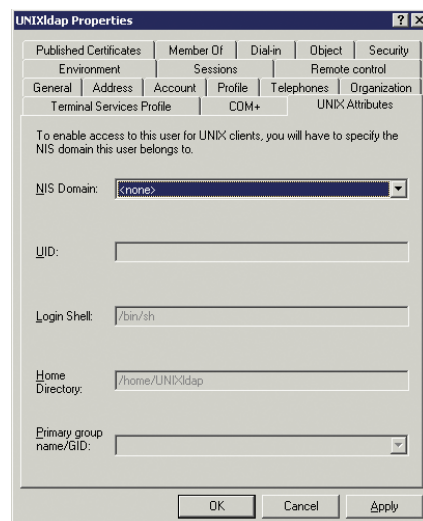
Необходимо отметить, что возможно два сценария обновления, в зависимости от того, установлен у вас пакет SFU или нет. Мы будем рассматривать вариант, при котором SFU не установлен. В противном случае рекомендую посетить англоязычный ресурс <http://www.winlinanswers.com/book/resources.php?id=5>, где вы найдете полное описание варианта обновления до R2 с установленным SFU.

Вставив CD#2 с дистрибутивом Windows Server 2003 R2 и согласившись на продолжение установки, вы увидите сообщение об ошибке с описанием, что установка не может быть продолжена, поскольку версия схемы данного домена не совместима с R2. Поэтому сначала необходимо выполнить следующую команду:

```
X:\COMPONENTS\R2\ADPREP\adprep.exe /forestprep
```

где X – буква, соответствующая CD с дистрибутивом. После чего можно начать установку компонентов R2, выполнив файл R2auto.exe из корневой директории CD.

После установки компонентов R2 нужно в панели управления в разделе



Свойства UNIX-пользователя - UNIX attributes

установки и удаления программ выбрать пункт «Windows Components», затем найти строчку «Active Directory Services» и в детализации выбрать установку «Identity Management for UNIX».

После завершения установки необходимо будет перезагрузить сервер.

### Настройка атрибутов будущих UNIX-пользователей и групп

Откройте оснастку Active Directory User and Computers и вызовите свойства любого пользователя. Появилась новая закладка UNIX Attributes, в которой возможно назначить свойства UNIX-пользователя (см. рисунок). Для начала нам нужно создать несколько UNIX-групп, которые пригодятся нам в дальнейшем.

Создайте группу UNIXusers – это будет группа по умолчанию для всех UNIX-пользователей. Для этого создайте обычным способом группу нужного вам вида (Domain Local или Global), затем откройте свойства данной группы и перейдите на вкладку «UNIX Attributes». В строке «NIS Domain» выберите ваш домен, после чего группе автоматически будет присвоен GID. Если он не устраивает вас по какой-то причине, можете прописать новый идентификатор вручную. При создании следующих групп GID будет автоматически увеличиваться на единицу.

Аналогичным способом создайте группу UNIXadmins, которая затем будет указана в настройках конфи-

группационного файла `/etc/sudoers` как группа, членам которой разрешено выполнять `sudo` на рабочих станциях с Kubuntu.

Создайте еще одну группу и назовите ее `audio`, присвоив ей вручную GID 29. Дело в том, что в Linux есть одна особенность – файлы аудиоустройств, как правило, имеют общую группу таким образом, что возможность работы с аудио доступна только владельцам файлов и членам этой группы. В эту группу потом добавим всех пользователей, чтобы у них была возможность использовать наушники и микрофон.

Теперь выберите одного из тех пользователей вашего домена, которому вы хотите присвоить UNIX-атрибуты. В свойствах откройте вкладку «UNIX Attributes», так же как и для группы, выберите имя вашего домена в строке «NIS Domain», и в строке «Primary group name/GID» выберите группу по умолчанию `UNIXusers`.

Если необходимо по каким-то причинам изменить параметры Login Shell и Home Directory, можно это сделать. UID присвоится автоматически, но при желании можно прописать его вручную.

После присвоения UNIX-атрибутов всем нуждающимся в них пользователям вернемся к группам. Открыв свойства группы `UNIXusers`, на вкладке «UNIX Attributes» нажмите кнопку «Add» и добавьте туда всех пользователей.

Аналогично поступим с группой `audio`, а в группу `UNIXadmins` внесем только тех пользователей, кому разрешено выполнение `sudo` на рабочих станциях.

Теперь остается только создать нового пользователя, например `unixldap`, и присвоить ему соответствующие атрибуты. Учетная запись этого пользователя будет использоваться при регистрации и поиске в LDAP с Linux-деSKTOPа, поэтому её необходимо максимально ограничить в правах, допустим, явно запретив доступ ко всем ресурсам файлового сервера и т. д.

На этом работы с оснасткой «Active Directory User and Computers» закончены.

## Немного о настройке файлового сервера для работы с UNIX-клиентами

В данном примере монтирование домашних каталогов пользователей осуществляется с использованием CIFS (Common Internet File System).

Если для каких-нибудь задач вам потребуется работа с NFS (Network File System), то для обеспечения доступа к файловым ресурсам вашего Windows-сервера с Linux-деSKTOPов необходимо будет установить на сервер пакет Microsoft Services for NFS. Привожу краткое руководство, как это сделать.

Зайдите в панель управления, затем в разделе установки и удаления программ выберите пункт «Windows Components», там войдите в «Other Network File and Print Services» и в детализации выберите установку «Microsoft Services for NFS». Из данного пакета необязательными к установке являются два последних пункта: Server for NFS Authentication и User Name Mapping. После установки данных служб пользователи с рабочих станций под управлением Linux получают доступ к файловым ресурсам данного сервера, используя NFS.

## Настройка рабочей станции с Kubuntu

Теперь приступим к самой большой части работы – настройке Kubuntu. Сначала выполните установку Kubuntu 7.10 на рабочую станцию, после чего установите все необходимые обновления, например, используя встроенный в KDE менеджер обновлений Adept Updater.

Также рекомендуется изменить параметры входа в систему для KDE (в других экранных менеджерах могут быть отличия) – открываем меню «System Settings», переходим на закладку «Advanced», там выбираем «Менеджер входа в систему», и, войдя в административный режим, отключаем опцию «Показывать список» на вкладке «Пользователи». Если этого не сделать, система при входе будет отображать всех UNIX-пользователей вашего домена, что совершенно ни к чему.

Для корректной работы протокола Kerberos, который будет использоваться для аутентификации в нашей гетерогенной среде, крайне важным моментом является синхронизация времени рабочей станции с контроллером домена.

Поэтому первым пунктом настроим синхронизацию времени. Для этого в файле `/etc/default/ntpdate` внесем следующие изменения:

```
NTPSERVERS="dc.domain.ru"
```

При следующей перезагрузке ПК будет синхронизировать время с контроллером домена, а пока проведем синхронизацию вручную, выполнив следующую команду:

```
$sudo ntpdate -s dc.domain.ru
```

Указываем FQDN для настраиваемой рабочей станции в файле `/etc/hosts`:

```
127.0.0.1 workstation.domain.ru localhost workstation
```

Проверьте доступность машины по FQDN командой:

```
ping workstation.domain.ru -c 4
```

Теперь необходимо установить и настроить поддержку Kerberos. Устанавливаем нужные пакеты:

```
$sudo apt-get install krb5-user libpam-krb5 \
krb5-config libkrb53 krb5-doc
```

Если система выдала ошибку:

```
dpkg was interrupted, you must manually run dpkg --configure -a
to correct this problem
```

последуйте совету подсказки, наберите:

```
$sudo dpkg --configure -a
```

В процессе вас попросят принять решение о замене файла `/etc/qt3/qt_plugins_3.3rc` – согласитесь с вариантом по умолчанию, оставьте текущую версию без изменений. Данная ошибка иногда проявляется в версии 7.10 после первой установки обновлений.

И приступаем к настройке – внесем изменения в файл `/etc/krb5.conf`:



```
[libdefaults]

default_realm = DOMAIN.RU
# DOMAIN.RU пишется обязательно ЗАГЛАВНЫМИ БУКВАМИ
ticket_lifetime = 24000

# 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
plain = {
something = something-else
}
fcc-mit-ticketflags = true

[realms]
DOMAIN.RU = {
kdc = dc.domain.ru
# kdc - key distribution center - контроллер домена
admin_server = dc.domain.ru
default_domain = domain.ru
}

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

[login]
krb4_convert = true
krb4_get_tickets = false

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log
```

После настройки Kerberos мы можем проверить его работоспособность следующими командами:

```
$kinit user@DOMAIN.RU
```

Командой kinit мы осуществляем запрос на сервер kdc на получение билета. Если система в ответ не выдала ошибок, значит, все в порядке и можно просмотреть билет командой klist:

```
$klist
```

```
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: user@DOMAIN.RU

Valid starting Expires Service principal
03/15/08 15:15:55 03/15/08 21:55:55 krbtgt/ DOMAIN.RU@DOMAIN.RU
```

Удалить билет можно командой kdestroy.

Если при выполнении команды kinit система выдала ошибку, проверьте настройки DNS, большинство проблем возникает именно из-за некорректной работы данной службы.

Далее на очереди установка и настройка поддержки LDAP:

```
$sudo apt-get install libnss-ldap libpam-ldap
```

При установке этих модулей вам сразу будет предложено настроить параметры клиента ldap, проигнорируйте это предложение, т.к. этих настроек будет недостаточно для корректной работы и все конфигурационные файлы надо настраивать вручную.

Изменяем файл /etc/ldap.conf:

```
# LDAP Defaults

# See ldap.conf(5) for details
# This file should be world readable but not world writable

uri ldap://dc.domain.ru
base dc=domain,dc=ru
ldap_version 3
scope sub
# Следующие две строки содержат реквизиты учетной записи
# unixldap, необходимые для доступа к схеме AD
binddn cn=unixldap,cn=Users,dc=domain,dc=ru
bindpw password
bind_timelimit 2
bind_policy soft
# bind_policy soft указывает, что при неудачном подключении
# к LDAP не пытаться переподключиться при отсутствии
# данной строки система не сможет загрузиться
idle_timelimit 2

# PAM options with group-based access configuration:
pam_filter objectClass=posixAccount
pam_login_attribute uid

# nsswitch.conf options:
nss_base_password cn=Users,dc=domain,dc=ru?sub
nss_base_group cn=Users,dc=domain,dc=ru?sub

# Далее прописываем mapping POSIX атрибутов,
# т.к. в схеме AD они не добавляются
nss_map_objectclass posixAccount User
nss_map_attribute homeDirectory unixHomeDirectory
nss_map_attribute gecos cn
nss_map_objectclass posixGroup Group

ssl no

# sudo options:
sudoers_base cn=UNIXadmins,cn=Users,dc=domain,dc=ru

# debug 257
```

Опцию debug можно будет включить на время отладки, если будут проблемы.

Также необходимо внести изменения в файл /etc/ldap/ldap.conf, который требуется для работы некоторых утилит, например ldapsearch. Это файл может состоять всего из двух строк:

```
BASE dc=domain,dc=ru
URI ldap://dc.domain.ru
```

Пришла очередь установить компоненты, которые позволят монтировать личные папки пользователей, располагающиеся на сервере Windows. Это пакеты smbfs и pam\_mount. Первый позволяет понимать windows share, а второй отвечает за автоматический mount/umount при процедурах login/logout. Устанавливаем:

```
$sudo apt-get install smbfs
```

А вот установка pam\_mount не отличается простой. Дело в том, что при установке с помощью команды «apt-get install» по умолчанию установится версия 0.18, которая не отличается дружелюбием по отношению к файловой системе cifs (хотя заявлено, что поддерживает), поэтому нам нужно установить более новую версию, например 0.32, а для этого придется обновить много библиотек и установить несколько пакетов. Итак, приступим. Скачайте следующие установочные файлы и установите их именно в такой последовательности:

- tzdata\_2008a-0ubuntu0.7.10\_all.deb
- libc6\_2.7-6\_i386.deb
- libhx10\_1.10.2-2\_i386.deb
- libssl0.9.8\_0.9.8g-4ubuntu1\_i386.deb

Теперь привычным способом установим пакет libxml-writer-perl:

```
$sudo apt-get install libxml-writer-perl
```

И только после всех описанных манипуляций скачиваем и устанавливаем пакет libpam-mount\_0.32-4\_i386.deb.

Конфигурационный файл модуля pam\_mount называется pam\_mount.conf.xml и находится в каталоге /etc/security. Я приведу здесь только измененные части файла, т.к. целиком его приводить смысла не имеет.

Для начала включим отладку:

```
<debug enable="1" />
```

Ниже перед закомментированным абзацем с описанием mntoptions вставим строчку:

```
<mntoptions allow="*" />
```

И наконец после строки:

```
<pmvarrun>pmvarrun -u %(USER) -o %(OPERATION)</pmvarrun>
```

вставляем свои строки с указанием следующих опций монтирования:

```
<volume
  user="*"
  invert="1"
  fstype="cifs"
  server="fileservr.domain.ru"
  path="/share/%(USER)"
  options="iocharset=utf8,dir_mode=0700,file_mode=0600"
  mountpoint="/home/%(USER)/data"
/>
```

Получается, что при входе в систему в домашнем каталоге пользователя будет создаваться папка /data, куда будет монтироваться его сетевая папка с сервера (\\fileservr.domain.ru\\share\\username).

Следующим шагом позаботимся о корректной работе sudo для соответствующих пользователей. Для этого внесем следующие изменения в файл /etc/sudoers:

```
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
%UNIXadmins ALL=(ALL) ALL
```

И еще изменим файл /etc/pam.d/sudo для корректной работы kdesu (запуск административных приложений в KDE):

```
##PAM-1.0
auth sufficient pam_krb5.so
auth sufficient pam_ldap.so          use_first_pass
auth sufficient pam_unix.so          use_first_pass
auth required pam_deny.so
#@include common-auth
#@include common-account
```

Теперь нам предстоит настроить модули PAM (Pluggable Authentication Modules) – подключаемые модули аутентификации. Описание принципов работы и синтаксис оставим за рамками нашей статьи, все интересующиеся без труда найдут его в сети. Изменениям подвергнутся несколько конфигурационных файлов, располагающихся в каталоге /etc/pam.d. Начнем с файла /etc/pam.d/common-account:

```
#account      required pam_login_access.so
account       required pam_ldap.so _
              ignore_authinfo unavail ignore_unknown_user
account       required pam_unix.so
```

Теперь редактируем файл /etc/pam.d/common-auth:

```
auth optional pam_mount.so
auth sufficient pam_krb5.so          use_first_pass
auth sufficient pam_ldap.so          ignore_authinfo _
unavail ignore_unknown_user use_first_pass
auth required pam_unix.so nullok_secure
auth required pam_deny.so
```

Следом вносим изменения в файл /etc/pam.d/common-password, который начнет работать только при смене пароля (по истечении срока или при запуске утилиты passwd):

```
password      sufficient pam_unix.so      obscure md5
password      sufficient pam_ldap.so
```

Переходим к файлу /etc/pam.d/common-session:

```
session optional      pam_mount.so
session               required pam_unix.so
session               optional pam_foreground.so
```

Необходимо отметить, что во всех модулях, использующих библиотеку pam\_mount, строчка с описанием ее использования должна быть на первом месте, к сожалению, pam\_mount не умеет принимать пароль через опции use\_first\_pass или try\_first\_pass, поэтому строка просто не работает, как следствие, сетевая папка не будет смонтирована.

Необходимо отметить, что указанные конфигурационные файлы работоспособны при осуществлении входа в систему через интерфейс KDE. Для использования консольного входа в систему (а также удаленного входа по ssh) нужно внести некоторые изменения, о которых подробно будет рассказано в описании настроек сетевых сервисов для сквозной авторизации.

На этом настройка модулей PAM завершена. Осталось внести изменения в последний, очень важный конфигурационный файл: /etc/nsswitch.conf:

```
group: files ldap
hosts: files dns
networks: files
passwd: files ldap
shells: files
sudoers: files ldap
```

Теперь остается только завершить сеанс и войти в систему под доменным UNIX-пользователем. При неудачной попытке ищите ошибки в log-файлах.

Настройка сетевых сервисов и служб для прозрачной и сквозной авторизации будет рассмотрена в следующий раз. 