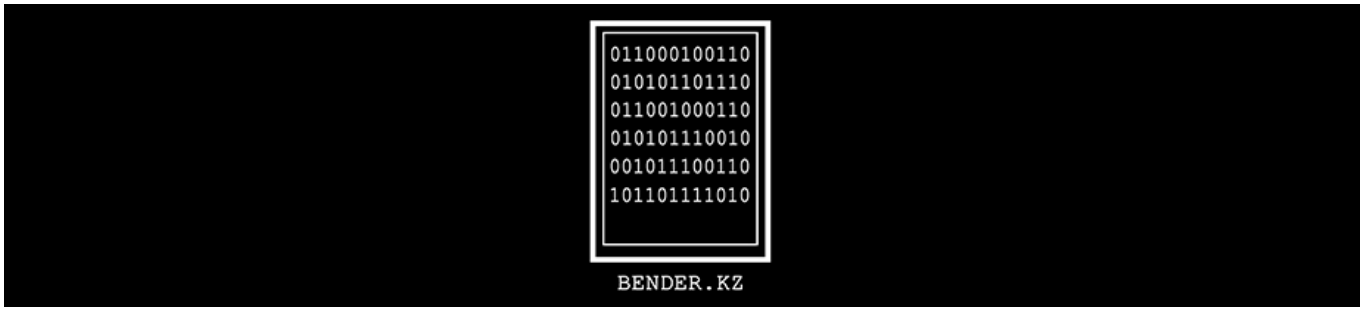
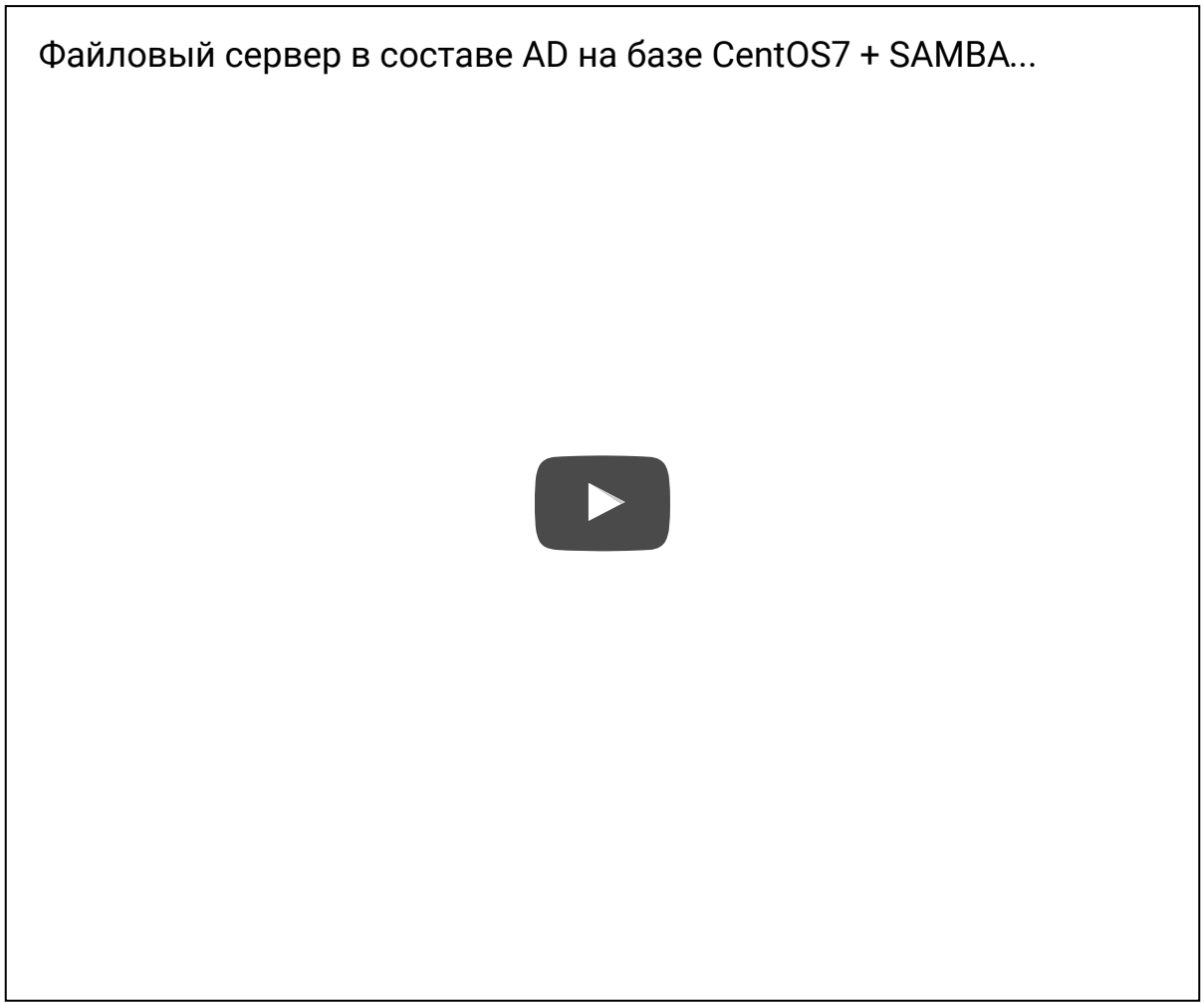


Файловый сервер в составе AD на базе CentOS7 + SAMBA



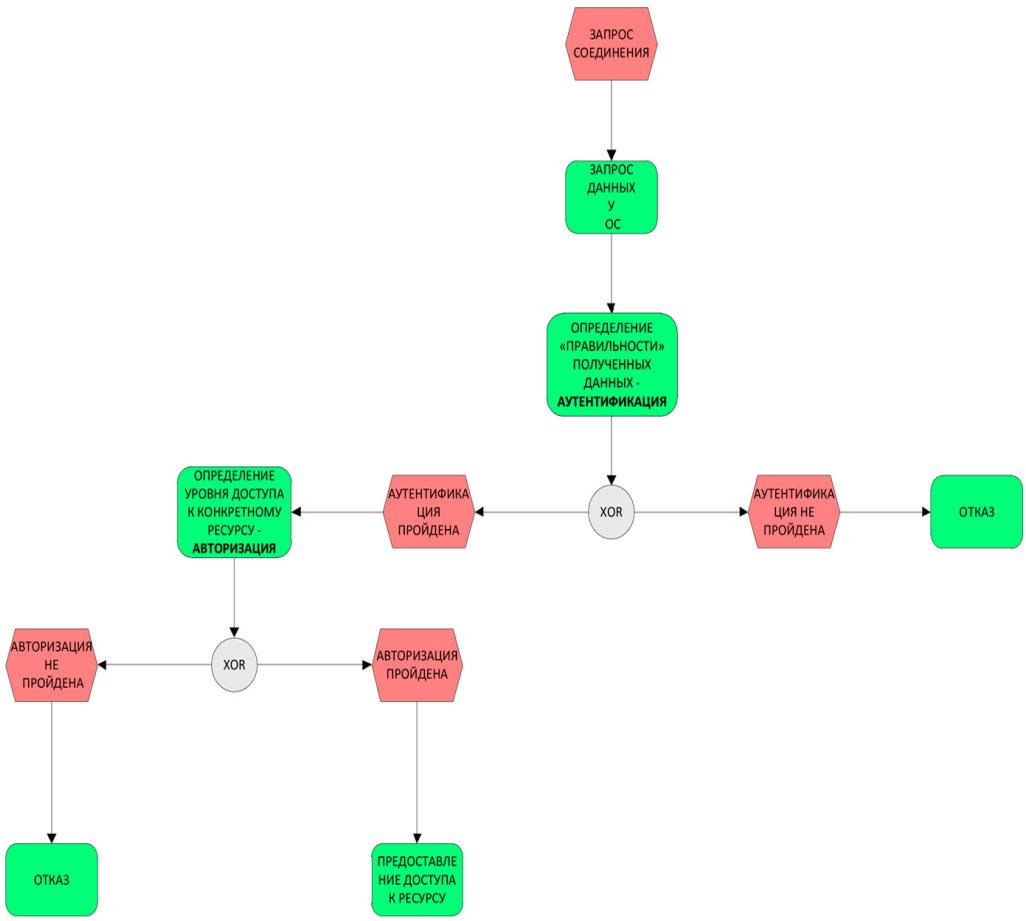
Сегодня мы с Вами поговорим о четвёртом сервере из нашей схемы – файловом сервере. Наш сервер мы будем разворачивать на базе программного комплекса SAMBA под управлением операционной системы CENTOS 7.

Сразу хочу сказать, что в такой конфигурации, как я покажу, сервер нельзя использовать для организации общего доступа к файловым базам, по крайней мере 1С версии 7.7. Там есть свои нюансы связанные с наложением блокировок на файл. Но о них мы поговорим, наверное когда я доберусь до темы с серверами 1С.

Ну, а сейчас давайте я более подробно расскажу, что будет представлять из себя наш файловый сервер. Как я уже говорил, для организации общего доступа к папкам, или, как часто все говорят, для настройки шар, мы воспользуемся уже известной нам по прошлым роликам SAMB'ой.

Для большинства админов, такая задача сводится к банальному щелчку по папке правой кнопкой мыши, и переходе к вкладке «ДОСТУП», это понятное дело в windows. О том, как работает сам механизм, многие не задумываются. Нам же с Вами придётся пойти по пути ДЖЕДАЯ и сделать несколько больше движений. Для того чтобы понять, что нам настраивать, давайте попробуем разобраться, как работает сам механизм доступа к общим папкам. Для этого, забежим немного вперёд и зайдём в нашу общую папку из windows. В принципе в этот момент произошло всего две вещи, это аутентификация – т.е. система убедилась в том, что введённые нами логин и пароль есть у неё в базе, и авторизация, т.е. система убедилась что нашему пользователю можно заходить в данную папку.

Теперь копнём глубже:



Файловый сервер, а в нашем случае это SAMBAслушает 445 порт по протоколу TCP. Затем, получив от клиента запрос на установку соединения происходит аутентификация, в процессе которой SAMBAобращается к операционной системе и проверяет есть ли предоставленные клиентом логин и пароль у неё в базе.

Если предоставленные данные в системе не найдены – аутентификация не проходит, и SAMBA сразу даёт отказ. Если данные есть – аутентификация прошла успешно. Далее начинается процесс авторизации.

Успешно аутентифицировавшись, клиент запрашивает доступ к нужной папке. Получив этот запрос SAMBA начинает смотреть, настройку разрешений конкретной папки и определять есть ли у данного пользователя доступ или нет. Если авторизация прошла успешно – то мы просто попадаем в папку.

Однако здесь нельзя забывать ещё и про файловую систему. Если на уровне файловой системы у Вас нет доступа хотя бы на просмотр – вы получите примерно следующее сообщение:

Этот, казалось бы, очевидный момент очень важен для новичков. Форумы просто завалены этим вопросом, хотя вроде бы всё очевидно.

Теперь, копнём ещё глубже и посмотрим, как работает система аутентификации:

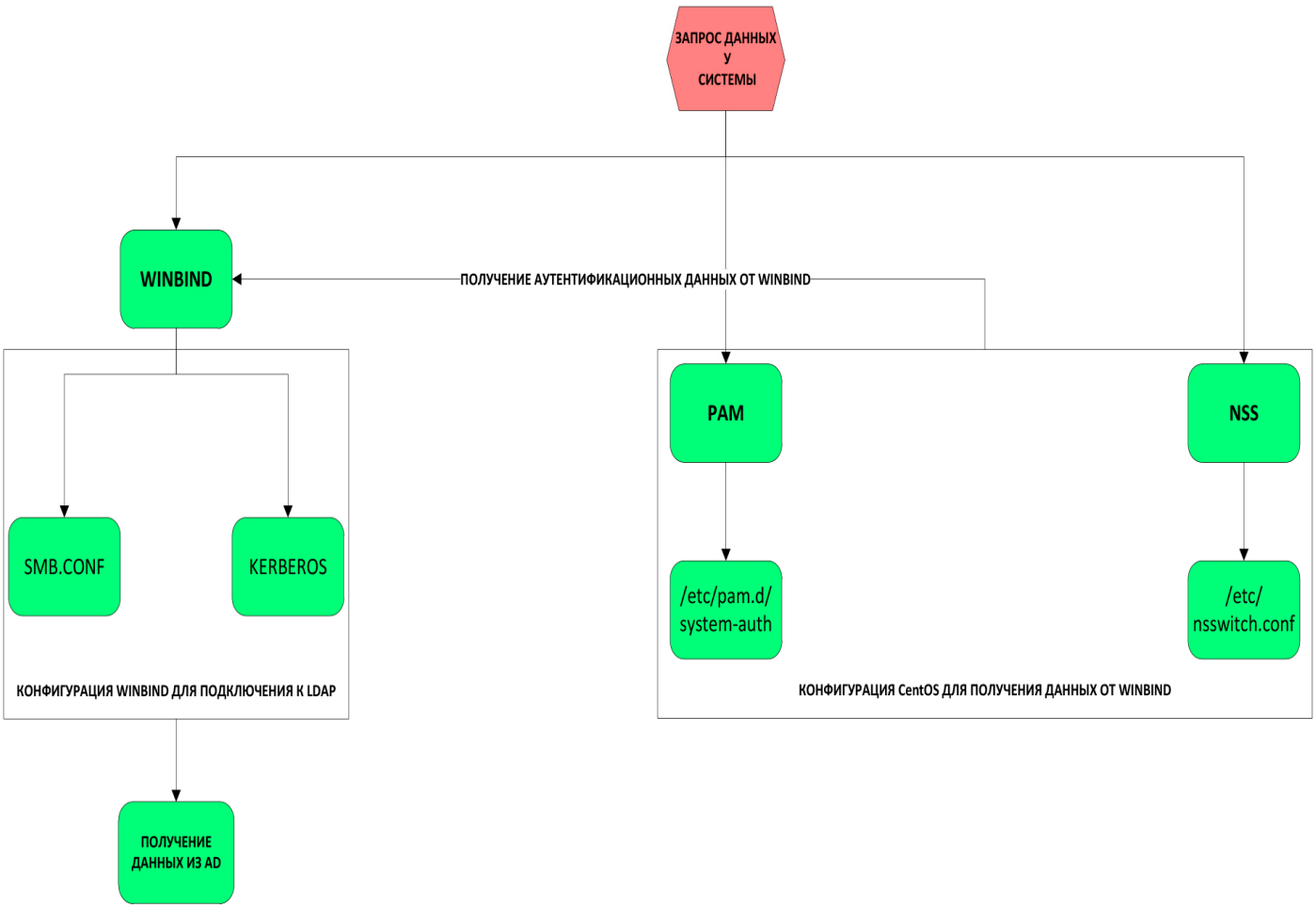
Рассмотрим процесс получения данных от системы. Точнее, что происходит в самой системе. Т.к. наш файловый сервер находится в домене, то и общие ресурсы предназначены для доменных пользователей. Сама по себе CentOS доступа к этим данным не имеет. Для того, чтобы их получить, нам понадобится пакет winbind. Он будет цепляться к LDAP-каталогу АД, получать данные об учётках, и по запросу передавать их в CentOS.

Как это происходит на деле описать будет трудно т.к. одновременно отрабатывает сразу несколько, тесно связанных между собой процессов, однако, я попробую:

Как я уже сказал, за получение данных о доменном пользователе отвечает winbind, для того, чтобы ему получить данные, нужно внести изменения в отдельную секцию файла настройки /etc/samba/smb.confи в керберос. После этого winbind, сможет зацепиться к нашему АД и получить данные.

А для того, чтобы система смогла получить данные от winbind'а, её тоже нужно соответствующим образом настроить. Нас интересуют две службы, это NSS (**name service switch**) и PAM (Pluggable Authentication). Эти службы тесно взаимосвязаны друг с другом. **NSS** – разрешает системе использовать в качестве источника аутентификационных данных программу winbind. Для её настройки нужно будет внести изменения в файл /etc/nsswitch, в то время, как **PAM**непосредственно производит процесс аутентификации, для её конфигурации мы внесём изменения в файл /etc/pam.d/system-auth

Теперь всё, что я сказал, попробуем разложить в некую, условную последовательность. Ещё раз обращаю Ваше внимание, что это условная последовательность, она нужна, лишь для того, чтобы Вы понимали, что и для чего мы настраиваем. Итак, поехали:



SAMBA запрашивает у ОСи аутентификацию пользователя. CentOS обращается к службе NSS, та считывает настройки из файла /etc/nsswitch.confи смотрит откуда ей можно брать данные. Далее начинает действовать PAM, она считывает файл /etc/pam.d/system-authи запрашивает у winbind'а существуют ли предоставленные пользователем данные. К этому времени winbind уже должен быть настронн и иметь доступ к LDAP каталогу нашего АД, а для этого должны быть отредактированы файлы /etc/samba/smb.conf и /etc/krb5.conf. И только после этого PAM вернёт SAMB'е ответ об успешной или неуспешной аутентификации текущего пользователя. Далее, SAMBAсогласно разрешениям для этого пользователя указанным в секции конкретной шары, в файле /etc/samba/smb.confпредоставит, либо запретит доступ.

Вот примерно, так это работает.

Давайте приступим непосредственно к настройке.

Обновляем ОС:

```
1 yum update -y
```

Выключаем SELinux:

```
vim /etc/selinux/config
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#    enforcing - SELinux security policy is enforced.
#    permissive - SELinux prints warnings instead of enforcing.
#    disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#    targeted - Targeted processes are protected,
#    minimum - Modification of targeted policy. Only selected processes are
protected.
#    mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Устанавливаем SAMBA и все пакеты необходимые для его работ:

```
yum install ntp acpid elinks acl bash-completion krb5-workstation samba samba-
winbind samba-winbind-clients samba-client samba-common wget vim ntpdate ntp mc -y
```

Создаём директории, которые будем использовать для общего доступа и даём им нужные права. Для примера я дам максимальные права:

```
mkdir /mnt/share
mkdir /mnt/share/admin
mkdir /mnt/share/public
mkdir /mnt/share/group
chmod 777 -R /mnt/share/
```

Убиваем, или копируем конфигурационный файл SAMB'ы. Хотя вообще-то лучше копировать…

```
rm /etc/samba/smb.conf
vim /etc/samba/smb.conf
```

Редактируем файл настроек SAMBA и WINBIND vim /etc/samba/smb.conf:

```
[global]
      workgroup = TRANING
      password server = DC.TRANING.KZ
      realm = TRANING.KZ
      security = ads
      idmap config * : range = 16777216-33554431
      template shell = /bin/bash
      kerberos method = secrets only
      winbind use default domain = true
      winbind offline logon = false
      winbind separator = +
      netbios name = files
      encrypt passwords = yes
      winbind nss info = rfc2307
      winbind trusted domains only = no
      winbind enum users  = yes
      winbind enum groups = yes
[public]
      comment = public
      path = /mnt/share/public
      browseable = yes
      read only = no
      create mask = 0664
      directory mask = 775
      admin users = @"TRANING+domain admins"
      valid users = @"TRANING+domain users"
[managers]
      comment = for manager
      path = /mnt/share/group
      valid users = @"TRANING+managers", @"TRANING+domain admins"
      admin users = @"TRANING+domain admins"
      read only = No
      create mask = 0664
      directory mask = 0775
[admin]
      comment = for admins only
      path = /mnt/share/admin
      browseable = yes
      read only = no
      create mask = 0664
      directory mask = 775
      valid users = @"TRANING+domain admins"
```

Итак секция [global] – т.е. глобальные настройки, от которых будет зависеть не только работы SAMBA но и WINBIND

- **workgroup = TRANING** – имя нашего домена
- **passwordserver = DC.TRANING.KZ** – сервер где лежит каталог LDAP
- **realm = TRANING.KZ** – имя нашего REALM'а
- **security = ads** – этот параметр указывает нужно ли smb-клиентам передавать данные для аутентификации или нет. Значение ads– означает, что сервер работает как член домена AD.
- **idmapconfig * : range = 16777216-33554431** – Этот параметр влияет на генерацию UIDи GID. Но т.к. в нашей сети планируется использовать только один файловый сервер SAMBA я его пропущу.
- **templateshell = /bin/bash** - Путь до оболочки, которую будут использовать пользователи утентифицированные через winbind
- **kerberos method = secrets only** – способ аутентификации kerberos
- **winbindusedefaultdomain = true** - Этот параметр разрешает winbindd (8) управлять пользователями без доменной части в имени пользователя. Пользователи без доменной части в имени рассматриваются winbindd сервером как принадлежащие текущему домену.
- **winbindofflinelogon = false** – Грубо говоря, этот параметр запрещает WINBIND хранить аутентификационные данные в кэше. Если выставить значение в true, winbindсохранит данные в кэше в завшифрованном виде.

- **winbindseparator = +** - Этот параметр указывает, какой вы будете использовать разделитель между DOMAINи USER. В моём случае – это знак плюса. Т.е. TRANING+user. Ниже это видно.
- **netbiosname = files** - Этот параметр указывает NETBIOS имя нашего сервера.
- **encryptpasswords = yes** - Этот параметр контролирует будет ли использоваться шифрование паролей между сервером и клиентом
- **winbindnssinfo = rfc2307** – этот параметр определяет, как winbind будет создавать домашние каталоги пользователей. Параметр rfc2307 – определяет, что данные будут браться непосредственно с LDAP каталога AD.
- **winbindtrusteddomainsonly = no**– честно говоря, не знаю как его описать своими словами, всем кому интересно заходите на сайт smb-conf.ru и смотрите в соответствующей секции.
- **winbind enum users = yes**
- **winbind enum groups = yes**

Эти два параметра отвечают за получение winbind'ом данных о пользователях и группах из LDAP каталога АД. Их, мы трогать не будем, просто оставьте их, как есть.

Ниже следуют секции конкретных шар.

[public] – шара для общего доступа всех пользователей домена

- comment = public – комментарий к ресурсу – тот.
- path = /mnt/share/public – физический путь до шары
- browseable = yes– Параметр указывает, будет ли общий ресурс отображаться в списке доступных общих ресурсов в сетевом окружении и в списке просмотра.
- readonly = no – если включить YES нельзя будет изменять файлы в этой директории
- createmask = 0664 – Это NIX'овые права на создаваемые файлы, на уровне файловой системе. В моём случае – владельцу и группе разрешены чтение и запись, остальным только чтение
- directorymask = 775 – Параметр аналогичен предыдущему, только применяется он к папкам.
- adminusers = @"TRANING+domainadmins" – Это полезный параметр. Он определяет пользователя или группу, которые в пределах данного ресурса будут обладать параметрами root'a. Т.е. полный доступ к любым файлам.
- validusers = @"TRANING+domainusers" – пользователи имеющие доступ к этому общему ресурсу.

Ниже идут секции других общих ресурсов, они, как Вы видите однотипны. Меняются только пользователи.

К ресурсу managers имеют доступ все кто в ходит в одноименную группу, а к ресурсу admin имеют доступ только администраторы домена.

Кстати администраторы домена имеют полный доступ ко всем ресурсам.

Закрываем и сохраняем файл, идём дальше.

Для правильной работы керберос необходимо настроить сервер времени, чтобы время на нашем сервере совпадало с временем сервера АД. Для этого правим файл /etc/ntp.conf Строчки с другими серверами мы комментируем, и добавляем адрес нашего сервера АД:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server dc.traning.kz
#server 0.centos.pool.ntp.org iburst
#server 1.centos.pool.ntp.org iburst
#server 2.centos.pool.ntp.org iburst
#server 3.centos.pool.ntp.org iburst
#broadcast 192.168.1.255 autokey      # broadcast server
#broadcastclient                   # broadcast client
#broadcast 224.0.1.1 autokey         # multicast server
#multicastclient 224.0.1.1           # multicast client
#manycastserver 239.255.254.254       # manycast server
#manycastclient 239.255.254.254 autokey # manycast client
# Enable public key cryptography.
#crypto
...
```

Теперь запустим принудительную синхронизацию командой ntpdateи адрес нашего сервера:

```
ntpdate dc.traning.kz
```

Включаем автозагрузку служб ntp, winbindи samba:

```
systemctl enable ntpd.service
systemctl enable winbind
systemctl enable smb.service
```

Добавляем в файрвол правила для работы samba:

```
firewall-cmd --permanent --add-service=samba
```

И перезагрузимся

```
reboot
```

Получаем керберос-билет:

```
[root@files ~]# kinit Administrator@TRANING.KZ
Password for Administrator@TRANING.KZ:
Warning: Your password will expire in 43 hours on Sat 14 Feb 2015 06:08:37 PM ALMT
```

Просмотрим его:

```
[root@files ~]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: Administrator@TRANING.KZ
Valid starting     Expires           Service principal
02/12/2015 22:20:52  02/13/2015 08:20:52  krbtgt/TRANING.KZ@TRANING.KZ
      renew until 02/19/2015 22:20:47
```

Теперь попробуем запустить wbinfoи посмотреть список доменных групп

```
wbinfo -g
```

Как видите в ответ мы получили ошибку, мы словили её потому, что не настроили PAM и NSS о которых я рассказывал раньше. Для того, чтобы их настроить, воспользуемся утилитой authconfig-tuiставим соответствующие галочки, жмём ОК

```
authconfig-tui
```

Попробуем получить список групп теперь:

```
[root@files ~]# wbinfo -g
allowed rodc password replication group
enterprise read-only domain controllers
denied rodc password replication group
read-only domain controllers
group policy creator owners
ras and ias servers
domain controllers
enterprise admins
domain computers
cert publishers
dnsupdateproxy
domain admins
domain guests
schema admins
domain users
dnsadmins
managers
```

Как видите, никаких проблем не возникло.

Теперь попробуем получить список пользователей, для этого просто меняем параметр на –u

```
wbinfo -u
```

Проверим, видит ли система наших доменных пользователей, как своих:

```
[root@files ~]# getent passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
chrony:x:998:997::/var/lib/chrony:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
administrator:*:16777216:16777216:Administrator:/home/TRANING/administrator:/bin/ba
bender:*:16777217:16777216:bender:/home/TRANING/bender:/bin/bash
krbtgt:*:16777218:16777216:krbtgt:/home/TRANING/krbtgt:/bin/bash
guest:*:16777219:16777217:Guest:/home/TRANING/guest:/bin/bash
```

Отлично, вот они наши пользователи.

Аналогично для групп:

```
[root@files ~]# getent group
...
allowed rodc password replication group:x:16777218:
enterprise read-only domain controllers:x:16777219:
denied rodc password replication group:x:16777220:krbtgt
read-only domain controllers:x:16777221:
group policy creator owners:x:16777222:administrator
ras and ias servers:x:16777223:
domain controllers:x:16777224:
enterprise admins:x:16777225:administrator
domain computers:x:16777226:
cert publishers:x:16777227:
dnsupdateproxy:x:16777228:
domain admins:x:16777229:administrator
domain guests:x:16777217:
schema admins:x:16777230:administrator
domain users:x:16777216:
dnsadmins:x:16777231:
managers:x:16777238:bender
```

Вот они.

Перезагрузим машинку.

```
reboot
```

На этом, всё ;-)