Mar 9 · 15 min read

Доменный контроллер Samba4 на CentOS

Пакет Samba позволяет организовать аналог контроллера домена Windows 2003/2008 на Linux системах. С выходом четвертой версии Samba появилась возможность использовать групповые политики и ряд других функций, стандартных для контроллеров на базе Microsoft Windows Server.

В качестве DNS-backend можно использовать BIND9_DLZ. Однако настройка в связке с ним является довольно трудоемкой и "сырой", поскольку в официальных версиях Samba4 отсутствует его поддержка. В то же время, Samba позволяет использовать свой штатный DNS-backend—SAMBA_INTERNAL, вполне пригодный для использования в небольших корпоративных сетях.

В данной заметке будет рассмотрено, как настроить AD DC в Samba4 на CentOS 7.2 Minimal при использовании штатного DNS-backend—Samba_Internal.

Настройка сети и hostname.

Как правило, настройки сети и hostname задаются при установке CentOS, но если требуется изменить:

Способ 1. Через мастер настройки Network Manager:

```
nmtui
```

Способ 2. Через редактирование текстовых конфигураций:

Опеределяем имя файла с конфигурацией интерфейса:

```
# nmcli dev status
DEVICE TYPE STATE CONNECTION
eno16777984 ethernet connected eno16777984
```

или

```
nmcli con sh
NAME                UUID
TYPE            DEVICE
eno16777984         c78d41cc-6eee-44d1-a77a-ba416e8e8727
802-3-ethernet
Wired connection 1  e23e01c4-7eb0-4018-89f0-2b9bf27d1427
802-3-ethernet
[root@dc ~]# ls -l /etc/sysconfig/network-scripts/ifcfg-
*
-rw-r--r--. 1 root root 321 Mar  4 09:02
/etc/sysconfig/network-scripts/ifcfg-eno16777984
-rw-r--r--. 1 root root 254 Sep 16 14:51
/etc/sysconfig/network-scripts/ifcfg-lo
-rw-r--r--. 1 root root 327 Mar  4 08:26
/etc/sysconfig/network-scripts/ifcfg-Wired_connection_1
```

Значит искомый файл: */etc/sysconfig/network-scripts/ifcfg-eno16777984*. Открываем:

```
nano /etc/sysconfig/network-scripts/ifcfg-eno16777984
```

У меня сетевых интерфейса два и настройки выглядят так:

```
HWADDR=00:0C:29:E4:6F:ED
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
IPV6_AUTOCONF=no
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=”Wired connection 1"
UUID=e23e01c4-7eb0-4018-89f0-2b9bf27d1427
ONBOOT=yes
IPADDR=192.168.1.202
PREFIX=32
GATEWAY=192.168.1.2
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
```

и

```
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
IPV6_AUTOCONF=no
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=eno16777984
UUID=c78d41cc-6eee-44d1-a77a-ba416e8e8727
DEVICE=eno16777984
ONBOOT=yes
DHCPV6C=yes
IPADDR=192.168.0.202
PREFIX=24
GATEWAY=192.168.0.1
IPV6_PRIVACY=no
DNS1=192.168.0.1
```

Учтите, что служба network парсит все, что лежит в данной папке и начинается с **ifcfg-***<имя_интерефейса>**, добавляя эти настройки ввиде дополнительных IP-адресов к данному адаптеру. Например, если создать два файла: *ifcfg-eno1* и *ifcfg-eno1–2,* то интерфейс будет иметь два айпи адреса и настройки содержащиеся в этих файлах.

Разобраться с настройками можно с помощью команды:

```
nmcli con sh
```

или

```
nmcli con sh <название интерфейса>
```

Зачастую при использовании AD DC в Samba возникают проблемы с поддержкой TCP/IP v6, поэтому отключаем поддержку :

```
echo net.ipv6.conf.all.disable_ipv6=1 >
/etc/sysctl.d/disableipv6.conf
```

Применяем настройки ядра:

```
sysctl -p
```

и перезапускаем сеть:

```
/etc/init.d/network restart
```

```
или:
```

```
service network restart
```

```
или:
```

```
systemctl restart network
```

Устанавливаем hostname:

```
# nano /etc/sysconfig/network
```

```
HOSTNAME=dc
```

Поумолчанию net-tools не включены в CentOS7 Minimal.
Устанавливаем, если нужно и проверяем настройки сети:

```
yum -y install net-tools
ifconfig -a
```

Отключение selinux.

```
# nano /etc/sysconfig/selinux
```

```
SELINUX=disabled
```

Применяем настройки без перезагрузки:

```
setenforce 0
```

Установка и настройка samba.

Самый простой способ—поставить из репозиториев. На текущий момент актуальная версия 4.2.3:

```
yum -y install samba samba-common
```

Собрав Samba из исходников, можно получить более свежую версию. Но вместе с тем это приносит ряд неудобств ввиде дополнительных настроек и ручного создания скриптов.

Нам потребуется:

```
# yum -y install gcc make wget python-devel gnutls-devel
openssl-devel libacl-devel krb5-server krb5-libs krb5-
workstation openldap-devel
```

На данный момент актуальной версией samba была 4.3.5. У меня в виртуальной машине выделено восемь ядер CPU, поэтому команды я буду вызывать с ключем *-j16*. Собираем из исходников:

```
cd /root/
wget http://ftp.samba.org/pub/samba/samba-4.3.5.tar.gz
tar -xzvf samba-4.3.5.tar.gz
cd ./samba-4.3.5
./configure --enable-selftest --with-systemd
make -j16
make -j16 install
```

Можно так же собрать из исходников с git, где обнвления бывают чуть чаще. На момент написания актуальной была версия 4.5.0pre1.

```
yum -y install git-core
git clone git://git.samba.org/samba.git samba-master
cd samba-master
./configure --enable-selftest --with-systemd
make -j16
make -j16 install
```

Поднимаем домен. Предполагается, что это первый контроллер домена в новом домене Active Directory.

Вариант 1.

```
/usr/local/samba/bin/samba-tool domain provision
```

И далее указываем:

> ***Realm [DOMAIN.LOCAL]:*** *(Enter)*
> ***Domain [DOMAIN]:*** *(Enter)*
> ***Server Role (dc, member, standalone) [dc]:*** *(Enter)*
> ***DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)[SAMBA_INTERNAL]:*** *(Enter)*
> ***DNS forwarder IP address (write 'none' to disable forwarding) [192.168.0.1]:*** *8.8.8.8*
> ***Administrator password:*** *<пароль>*
> ***Retype password:*** *<пароль>*

По завершению увидим:

```
Server Role: active directory domain controller
Hostname: dc
NetBIOS Domain: DOMAIN
DNS Domain: domain.local
DOMAIN SID: S-1-5-21-446678553-2474708993-1810639841
```

Вариант 2.

```
/usr/local/samba/bin/samba-tool domain provision --
realm=domain.local --domain=DOMAIN --adminpass <пароль>
server-role=dc --dns-backend=SAMBA_INTERNAL
```

Далеко не все параметры доступны в интерактивном режиме, как, например, использование бэкэнда **rfc2307,** позволяющего использовать POSIX-атрибуты (UID / GID) всхеме AD. Поэтому для использования rfc2307 необходимо вызывать команду с ключем:

```
--use-rfc2307
```

rfc2307 необходим при аутентификации BSD, Linux и OS X машин, в дополнении к Windows. rfc2307 определяет возможность хранить данные о пользователях и группах в каталоге LDAP, а не в специальном текстовом файле в отличае от *idmap_rid*. При использовании двух контроллеров доменов нужно использовать rfc2307. В случае если у вас два контроллера домена, вам придется использовать winbind backend = **ad**.

```
--use-ntvfs
```

use-ntvfs позволяет использовать файловый сервис NTVFS (по умолчанию в Samba4 включен именно он), или вы можете указать файловый сервис от Samba3—s3fs.

```
--use-xattrs=yes
```

use-xattrs позволяет расширенное использование атрибутов ACLs файлов, размещенных на linux машине. Файловые системы xfs и ext4 поддерживают эти параметры по умолчанию.

Любые из этих параметров можно изменить позже, добавив нужные строчки в smb.conf. С полным списком можно ознакомиться здесь.

Итак, запускаем Samba:

```
/usr/local/samba/sbin/samba
```

При компиляции Samba4 из исходников придется создать скрипт инициализации вручную:

```
nano /etc/init.d/samba4
```

и скопировать:

```
#! /bin/bash
#
# samba4 Bring up/down samba4 service
#
# chkconfig: — 90 10
# description: Activates/Deactivates all samba4
interfaces configured to
# start at boot time.
#
### BEGIN INIT INFO
# Provides:
# Should-Start:
# Short-Description: Bring up/down samba4
# Description: Bring up/down samba4
### END INIT INFO
# Source function library.
```

```
. /etc/init.d/functions
```

```
if [ -f /etc/sysconfig/samba4 ]; then
. /etc/sysconfig/samba4
fi


CWD=$(pwd)
prog="samba4"
```

```
start() {
# Attach irda device
echo -n $"Starting $prog: "
/usr/local/samba/sbin/samba
sleep 2
if ps ax | grep -v "grep" | grep -q /samba/sbin/samba ;
then success $"samba4 startup"; else failure $"samba4
startup"; fi
echo
}
stop() {
# Stop service.
echo -n $"Shutting down $prog: "
killall samba
sleep 2
if ps ax | grep -v "grep" | grep -q /samba/sbin/samba ;
then failure $"samba4 shutdown"; else success $"samba4
shutdown"; fi
echo
}
```

```
status() {
/usr/local/samba/sbin/samba — show-build
}


# See how we were called.
case "$1" in
start)
start
;;
stop)
stop
;;
status)
status irattach
;;
restart|reload)
stop
start
;;
*)
echo $"Usage: $0 {start|stop|restart|status}"
exit 1
esac
exit 0
```

Разрешаем его запуск:

```
chmod 750 /etc/init.d/samba4
```

При компиляции из ихсодников для того, чтобы зарегистрировать службу samba4 и добавить в автозагрузку необходимо так же создать файл:

```
# nano /etc/systemd/system/samba4.service
```

```
[Unit]
Description= Samba 4 Active Directory
After=syslog.target
After=network.target
[Service]
Type=forking
PIDFile=/usr/local/samba/var/run/samba.pid
ExecStart=/usr/local/samba/sbin/samba
[Install]
WantedBy=multi-user.target
```

и разрешить автозагрузку:

```
systemctl enable samba4
```

Далее проверяем аутентификацию NT:

```
# /usr/local/samba/bin/smbclient -L localhost -U%
```

Если все прошло успешно, то увидим:

```
Domain=[DOMAIN] OS=[Windows 6.1] Server=[Samba 4.3.5]
```

```
Sharename Type Comment
 – – – – – – – – – – -
 netlogon Disk
 sysvol Disk
 IPC$ IPC IPC Service (Samba 4.3.5)
Domain=[DOMAIN] OS=[Windows 6.1] Server=[Samba 4.3.5]
```

```
Server Comment
 – – – – – – – – – -
```

```
Workgroup Master
 – – – – – – – – – -
```

если нет—смотрим логи. Открываем */etc/resolv.conf*, добавляем туда адрес нашего DNS:

```
# nano /etc/resolv.conf
```

```
nameserver 127.0.0.1
```

и тестируем DNS:

```
host -t SRV _ldap._tcp.domain.local
host -t SRV _kerberos._udp.domain.local
host -t A dc.domain.local
```

если все успешно, то результат будет наподобие:

```
_ldap._tcp.domain.local has SRV record 0 100 389
dc.domain.local.
_kerberos._udp.domain.local has SRV record 0 100 88
dc.domain.local.
dc.domain.local has address 192.168.0.202
dc.domain.local has address 192.168.1.202
```

Правим smb.conf:

```
# nano /usr/local/samba/etc/smb.conf
```

```
# Global parameters
[global]
 workgroup = DOMAIN
 realm = domain.local
 netbios name = DC
 server role = active directory domain controller
 # если в DNS нет записей, то перенаправление на Google
Public DNS
 dns forwarder = 8.8.8.8
 # Don’t allow any updates | allow unsigned updates |
only signed updates
 # allow dns updates = False | nonsecure | signed
 allow dns updates = nonsecure
 # команда для обновления обратной и прямой зоны
 nsupdate command = /usr/bin/nsupdate -g


[netlogon]
 path =
/usr/local/samba/var/locks/sysvol/domain.local/scripts
 read only = No
 write ok = Yes
```

```
[sysvol]
 path = /usr/local/samba/var/locks/sysvol
 read only = No
 write ok = Yes
```

Добавляем линк на файл конфигурации kerberos:

```
ln -sf /usr/local/samba/private/krb5.conf /etc/krb5.conf
```

и сверяем настройки:

```
# nano /etc/krb5.conf
```

```
[libdefaults]
 default_realm = DOMAIN.LOCAL
 dns_lookup_realm = false
 dns_lookup_kdc = true
```

Тестируем:

```
kinit administrator@DOMAIN.LOCAL
```

вводим пароль и при правильных настрйках увидим что-то наподобие:

```
Password for administrator@DOMAIN.LOCAL:
Warning: Your password will expire in 41 days on Mon 18
Apr 2016 08:54:44 AM MSK
```

Нас уведомляют о том, что срок действия пароля истечет через 41 день. По мере необходимости при создании учетных записей можно менять значение на “Password never expires”, а можно сменить дефолтное значение на 999 дней:

```
/usr/local/samba/bin/samba-tool domain passwordsettings
set --max-pwd-age=999
```

Проверяем:

```
/usr/local/samba/bin/samba-tool domain passwordsettings
show | grep Max
```

Или вовсе сменить значение на бессрочное:

```
/usr/local/samba/bin/samba-tool domain passwordsettings
set --complexity=off --min-pwd-length=6 --max-pwd-age=0
```

Здесь помимо отключения срока действия пароля отменено требование к сложности пароля (complexity=off) и минимальная длина установлена в значение равное 6 символам (однако позже при создании пользователей через RSAT меня все равно попросило создать пароль точно такой же сложности, как и в MS Windows Server).

Проверяем полученный ticket для учетной записи Administrator:

```
# klist
```

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@DOMAIN.LOCAL
```

```
Valid starting Expires Service principal
03/08/2016 03:45:32 03/08/2016 13:45:32
krbtgt/DOMAIN.LOCAL@DOMAIN.LOCAL
 renew until 03/09/2016 03:45:25
```

Далее необходимо создать зону обратного просмотра для каждой подсети в среде DNS, поскольку она не создается автоматически:

```
/usr/local/samba/bin/samba-tool dns zonecreate
server.domain.local xxx.xxx.xxx.in-addr.arpa
```

где: xxx.xxx.xxx—первые три байта подсети в обратном порядке (например: 192.168.0.0/24 станет 0.168.192):

```
/usr/local/samba/bin/samba-tool dns zonecreate
dc.domain.local 0.168.192.in-addr.arpa
```

Теперь нужно добавить запись для сервера (если сервер multi-homed, то для каждой подсети):

```
/usr/local/samba/bin/samba-tool dns add
server.domain.local xxx.xxx.xxx.in-addr.arpa zzz PTR
server.domain.local
```

zzz будет замененён четвёртым октетом IP для сервера. Например:

```
/usr/local/samba/bin/samba-tool dns add dc.domain.local
0.168.192.in-addr.arpa zzz PTR dc.domain.local
```

Проверяем:

```
host -t PTR 192.168.0.202
```

Возможно, вы получите сообщение об ошибке вида:

```
Host 202.0.168.192.in-addr.arpa. not found: 3(NXDOMAIN)
```

но сама зона успешно создастся и будет видна в RSAT в менеджере DNS:

Предпологаю, это баг Samba и как с ним бороться мне пока что неизвестно.

Для того, чтобы каждый раз не вызывать Samba, используя полный путь, добавляем путь к samba в переменную PATH:

```
export
PATH=/usr/local/samba/bin/:/usr/local/samba/sbin/:$PATH
```

На этом основная настройка Samba завершена и можно вводить компьютеры в домен.

Установка и настройка ntp.

Сервер NTP требуется для аутентификации Kerberos. Если время будет неправильным клиенты не смогут пройти аутентификацию на сервере.

Устанавливаем:

```
yum -y install ntp
```

Открываем конфигурацию:

```
nano /etc/ntp.conf
```

и добавляем/меняем параметры:

```
server 0.pool.ntp.org     iburst prefer
```

```
driftfile /var/lib/ntp/drift
logfile /var/log/ntp
ntpsigndsocket /usr/local/samba/var/lib/ntp_signd/
```

```
server 127.127.1.0
fudge 127.127.1.0 stratum 10
```

```
restrict 127.0.0.1
restrict default kod nomodify notrap nopeer mssntp
restrict 0.pool.ntp.org mask 255.255.255.255 nomodify
notrap nopeer noquery
restrict 1.pool.ntp.org mask 255.255.255.255 nomodify
notrap nopeer noquery
```

Выставляем права и создаем линк:

```
chown root:ntp /usr/local/samba/var/lib/ntp_signd/
chmod 750 /usr/local/samba/var/lib/ntp_signd/

ls -ld /usr/local/samba/var/lib/ntp_signd/
```

Ставим правильный часовой пояс:

```
# nano /etc/sysconfig/clock
```

```
ZONE="Europe/Moscow"
UTC=false
ARC=true
```

далее:

```
mv /etc/localtime /etc/localtime.bak
ln -s /usr/share/zoneinfo/Europe/Moscow /etc/localtime
systemctl restart ntpd
```

и проверяем время:

```
date
```

Управление групповыми политиками.

Для того, чтобы управлять доменными политиками на введенном в домен компьютере под управлением Windows 7 устанавливаем RSAT (Remote Server Administration Tools for Windows 7 with Service Pack 1).

Заходим в панель управления, выбираем Programs and Features (Программы и компоненты) и далее—Turn Windows features on

or off. В разделе Remote Server Administration Tools -> Role Administration Tools выбираем **AD DS and AD LDS Tools**.

После этого консоль AUDC и другие оснастки появятся в панели управления в разделе Administrative Tools, а так же в Пуск -> Администрирование.

Чтобы активировать оснастки Active Directory Users and Computers после установки RSAT из командной строки нужно выполнить:

```
dism /online /enable-feature
/featurename:RemoteServerAdministrationTools-Roles-AD-DS

dism /online /enable-feature
/featurename:RemoteServerAdministrationTools-Roles-AD-
DS-SnapIns
```

Однако при этом все равно необходимо установить RSAT.

Настройка SSL.

Active Directory испльзует LDAP (Lightweight Directory Access Protocol), шифрование которого по умолчанию отключено. Для обеспечения безопасности необходимо включить SSL/TSL. Сам сертификат был уже создан, когда поднимался домен:

> */usr/local/samba/private/tls/ca.pem*
> */usr/local/samba/private/tls/cert.pem*

> */usr/local/samba/private/tls/key.pem*

Поумолчанию сертификаты действительны в течение 700 дней с момента их создания. Чтобы использовать их в конфигурацию Samba следует добавить строки:

```
# nano /usr/local/samba/etc/smb.conf
```

```
[global]
        tls enabled = yes
        tls keyfile = tls/key.pem
        tls certfile = tls/cert.pem
        tls cafile = tls/ca.pem
```

и перезапустить Samba:

```
service samba4 restart
```

Использование самозаверяющегося (self-signed) сертификата.

```
# cd /usr/local/samba/private/tls/
```

Создайте ключь длинной 2048 байт сроком действия 9999 дней. Заполните все поля, особенно FQDN-имя вашего контроллера-домена:

```
# openssl req -newkey rsa:2048 -keyout myKey.pem -nodes
-x509 -days 9999 -out myCert.pem
```

```
Generating a 2048 bit RSA private key
.............+++
..+++
writing new private key to 'myKey.pem'
-----
You are about to be asked to enter information that will
be incorporated
into your certificate request.
What you are about to enter is what is called a
Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some
blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:RU
State or Province Name (full name) []:My City
Locality Name (eg, city) [Default City]:My Location
Organization Name (eg, company) [Default Company Ltd]:My
Company
Organizational Unit Name (eg, section) []:My Unit
Common Name (eg, your name or your server's hostname)
[]:dc.domain.local
Email Address []:myemail@email.com
```

Далее следует задать права:

```
# chmod 600 myKey.pem
```

добавить строки в конфигурацию:

```
# nano /usr/local/samba/etc/smb.conf
```

```
[global]
tls enabled  = yes
tls keyfile  = tls/myKey.pem
tls certfile = tls/myCert.pem
tls cafile   =
```

и перезапустите Samba:

```
service samba4 restart
```

Использование доверенного (trusted) сертификата.

```
# cd /usr/local/samba/private/tls/
# openssl genrsa -out myKey.pem 2048
```

Аналогично заполняем поля. Важно задать в поле “Common Name” FQDN домен контроллра (*hostname -f*). Добавляем строки в конфигурацию:

```
# nano /usr/local/samba/etc/smb.conf
```

```
[global]
tls enabled  = yes
tls keyfile  = tls/myKey.pem
tls certfile = tls/myCert.pem
tls cafile   = tls/myIntermediate .pem  #не заполнять,
если не требуется
```

и перезапускаем Samba.

Проверка сертификата.

Просмотреть данные о сертификате можно следюущей командой:

```
# openssl x509 -in
/usr/local/samba/private/tls/myCert.pem -noout -text
```

Проверка сертификата локально:

```
# openssl verify /usr/local/samba/private/tls/myCert.pem
```

Есть используется CA, то используйте команду:

```
# openssl verify /usr/local/samba/private/tls/myCert.pem
-CApath /usr/local/samba/private/tls/ca-file.pem
```

Проверка сертфиката удаленно через TCP:

```
# openssl s_client -showcerts -connect
dc.domain.local:636
```

Если используется, CA, то:

```
# openssl s_client -showcerts -connect localhost:636 -
CApath /usr/local/samba/private/tls/ca-file.pem
```

Настройка iptables.

После того как настройка и тестирование завершены можно задать правила и включить iptables. Но для начала убедимся, что альтернативный firewalld отключен:

```
systemctl status firewalld
```

если активен, то убираем из автозагрузки и отключаем:

```
systemctl disable firewalld && systemctl stop firewalld
```

По желанию можно так же отключить Network Manager (команда *nmtui*), поскольку все настройки сети можно производить, редактируя */etc/sysconfig/network-scripts/*.

Проверяем статус Network Manager:

```
systemctl --type=service | grep NetworkManager
```

убираем из автозагрузки и отключаем:

```
systemctl disable NetworkManager && systemctl stop
NetworkManager
```

Для Enterprise Linux, возможно, потребуется убрать из автостарта ipchains:

```
service ipchains stop && chkconfig --level 345 ipchains
off
```

В минимальных дистрибутивах, таких как Centos 7.2 minimal пакет iptables поумолчанию может отсутствовать. Устанавливаем:

```
yum -y install iptables iptables-services
```

и добавляем правила:

```
# nano /etc/sysconfig/iptables
```

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
# дотсуп по SSH
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -
j ACCEPT
# DNS-запросы
-A INPUT -m state --state NEW -m udp -p udp --dport 53 -
j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 53 -
j ACCEPT
# Kerberos-авторизация
-A INPUT -m state --state NEW -m tcp -p tcp --dport 88 -
j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 88 -
j ACCEPT
# NTP
-A INPUT -m state --state NEW -m udp -p udp --dport 123
-j ACCEPT
# RPC, ECM, DHCP, DNS, WINS
-A INPUT -m state --state NEW -m tcp -p tcp --dport 135
-j ACCEPT
# NetBIOS
-A INPUT -m state --state NEW -m tcp -p tcp --dport 139
-j ACCEPT
-A INPUT -m state --state NEW -p udp -m multiport --port
137:138 -j ACCEPT
# LDAP-запросы от клиента к серверу
-A INPUT -m state --state NEW -m tcp -p tcp --dport 389
-j ACCEPT
```

```
-A INPUT -m state --state NEW -m udp -p udp --dport 389
-j ACCEPT
# SMB CIFS (File Replication Service)
-A INPUT -m state --state NEW -m tcp -p tcp --dport 445
-j ACCEPT
# KPASSWD (для смены пароля Kerberos)
-A INPUT -m state --state NEW -m tcp -p tcp --dport 464
-j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 464
-j ACCEPT
# LDAP с шифрованием по SSL или TSL
-A INPUT -m state --state NEW -m udp -p udp --dport 636
-j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 636
-j ACCEPT
# Dynamic RPC Ports
-A INPUT -m state --state NEW -m tcp -p tcp -m multiport
--port 1024:5000 -j ACCEPT
-A INPUT -m state --state NEW -p udp -m multiport --port
3268:3269 -j ACCEPT
# DNS Multicast
-A INPUT -m state --state NEW -m tcp -p tcp --dport 5353
-j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 5353
-j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Запускаем iptables и добавляем в автозагрузку:

```
systemctl start iptables.service
systemctl enable iptables.service
```

Листинг всех правил с номерами строк и портов можно получить по команде:

```
iptables -n -L -v --line-numbers
```

Создание общих файловых ресурсов.

Рассмотрим пример подключения раздела и создание CIFS (или сетевой share для Windows Networking) через Samba. Просмотрим список устройств:

```
# lsblk
```

```
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
fd0 2:0 1 4K 0 disk
sda 8:0 0 16G 0 disk
├─sda1 8:1 0 500M 0 part /boot
└─sda2 8:2 0 15.5G 0 part
 ├─centos_dc-root 253:0 0 15G 0 lvm /
 └─centos_dc-swap 253:1 0 512M 0 lvm [SWAP]
sdb 8:16 0 200G 0 disk
sr0 11:0 1 603M 0 rom
```

Возможны два варианта: создать раздел ext4 и примонтировать его, или расширить дисковое пространство через LVM. Оба метода расписаны здесь. Я буду использовать первый, поскольку он более однозначный: данные пишутся туда, куда примонтирован жесткий диск. К тому же, этот метод работает на любой сборке Linux.

```
fdisk -c -u /dev/sdb
```

Вводим **n**, отвечаем на вопросы и сохраняем изменения при вводе **w**:

```
Welcome to fdisk (util-linux 2.23.2).
```

```
Changes will remain in memory only, until you decide to
write them.
Be careful before using the write command.


Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier
0xf51d5d85.
```

```
Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-419430399, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-419430399,
default 419430399):
Using default value 419430399
Partition 1 of type Linux and of size 200 GiB is set
```

```
Command (m for help): w
The partition table has been altered!
```

```
Calling ioctl() to re-read partition table.
Syncing disks.
```

На созданном разделе */dev/sdb1* создаем файловую систему и присваиваем метку SHAREDATA:

```
mkfs.ext4 -L SHAREDATA /dev/sdb1
```

Реузльтатом будет что-то наподобие:

```
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=SHAREDATA
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
13107200 inodes, 52428544 blocks
2621427 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2199912448
1600 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
 32768, 98304, 163840, 229376, 294912, 819200, 884736,
1605632, 2654208,
 4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting
information: done
```

Список разделов можно посмотреть набрав команду:

```
fdisk -l
```

Создаем папку и монтируем в нее:

```
cd /media/ && mkdir share && mount /dev/sdb1
/media/share
```

Для того, чтобы использовать вкладку “безопасность” в свойствах папок в Windows требуется установаить расширенные атрибуты файлов и наследование прав доступа для Samba. Установим необходимое:

```
yum -y install acl attr
```

Перемонтируем файловую систему с нужными атрибутами:

```
mount -o remount,acl,user_xattr /dev/sdb1
```

Далее, чтобы монтирование происходило с нужными атрибутами по умолчанию, необходимо включить их поддержку на файловой системе:

```
tune2fs -o user_xattr,acl /dev/sdb1
```

Проверим присутствие атрибутов:

```
tune2fs -l /dev/sdb1 | grep "Default mount options"
```

Для того чтобы раздел автоматически монтировался при загрузке:

```
echo "/dev/sdb1 /media/share ext4
rw,relatime,data=ordered 0 0" >>   /etc/fstab
```

Или как вариант: нужную строчку можно просто скопировать из */etc/mtab* в */etc/fstab*.

Для того, чтобы эта папка стала доступна в сетевом окружении (CIFS или Windows Networking) нашего домена:

```
# nano /usr/local/samba/etc/smb.conf
```

```
[share]
 path = /media/share
 read only = No
 write ok = Yes
 browseable = yes
 guest ok = no
 public = yes
```

Перезапускаем samba:

```
service samba4 restart
```

После чего папка будет доступна в сетевом окружении Windows:

\\DC\share

PS.

Если ваш доменный контроллер работает стабильно уже несколько недель, то настройка завершена. Однако в некоторых случаях, особенно, если вы компилировали release condidate версии может потребоваться периодический перезапуск службы Samba. Проще всего поставить перезапуск службы каждый день в ночное время через crontab.

```
# crontab -e
```

При первом запуске утилита потребует выбрать вас редактор. Далее фомат записи будет следующим:

```
минута час день месяц день_недели команда
```

Минута—время в минутах от 0 до 59
Час—от 0 до 23
День—день месяца от 1 до 31
Месяц—от 1 до 12 либо буквенные обозначения jan—dec
День недели—от 0 до 6 (0—воскресенье) или sat—sun
Команда—строка в формате командного интерпретатора. Допускается запись типа **команда1 && команда2**.

Для того чтобы Samba перезапускалась каждый день в час ночи добавьте:

```
0 1 * * * systemctl restart samba4
```

И еще один момент: при использовании в качестве DNS-бэкенда SAMBA_INTERNAL, возможно, прямую зону DNS (узел A) для каждого компьютера придется добавлять вручную. Во всяком случае, я пока не нашел способа как обновлять их автоматически: