

РАЗДЕЛ 2 ПРАКТИЧЕСКАЯ ЧАСТЬ

ГЛАВА 1 РАЗВЕРТЫВАНИЕ СЕРВЕРА SAMBA НА ОПЕРАЦИОННОЙ СИСТЕМЕ ARCH LINUX

Данная глава посвящена установке дистрибутива Arch Linux, а также установке и конфигурации контроллера домена Samba на данном дистрибутиве.

1.1 Установка Arch Linux

Данный дистрибутив был выбран в качестве сервера Samba, так как он имеет обширную библиотеку знаний (archwiki), современные версии пакетов, а также, в данном дистрибутиве будут функционировать только те программы, которые вручную загрузит пользователь. Была осуществлена загрузка образа ISO, запись образа на flash-накопитель, и дальнейший вход в окружение установки. С помощью утилиты fdisk были отформатированы разделы жесткого диска в котором будет произведена дальнейшая установка. Раздел /dev/sda1 – основной раздел. Раздел /dev/sda2 – swap file (рис. 1).

```
root@archiso ~ # fdisk -l
Disk /dev/sda: 30 GiB, 32212254720 bytes, 62914560 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xdb12ce8e

Device      Boot   Start      End  Sectors  Size Id Type
/dev/sda1                7815168 62914559 55099392 26.3G 83 Linux
/dev/sda2                2048    7815167   7813120   3.7G 82 Linux swap / Solaris

Partition table entries are not in disk order.

Disk /dev/loop0: 496.6 MiB, 520732672 bytes, 1017056 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
root@archiso ~ # _
```

Рисунок 1 – Форматирование разделов жесткого диска

С помощью утилиты `mkfs.ext4` была создана файловая система для основного раздела.[17] С помощью `mkswap` был создан файл подкачки. С помощью утилиты `pacstrap` были установлены все необходимые пакеты (рис. 2), такие как:

- 1) `base` – основные утилиты GNU/Linux для управления файлами и системой.
- 2) `Base-devel` – набор утилит для сборки программ из источников.
- 3) `gnome` – графическая оболочка.
- 4) `vim` – текстовый редактор.
- 5) `grub` – начальный загрузчик.
- 6) `sudo` – утилита для выполнения команд с привилегиями администратора.

```
root@archiso ~ # mkfs.ext4 /dev/sda1
mke2fs 1.45.0 (6-Mar-2019)

Creating filesystem with 6887424 4k blocks and 1725136 inodes
Filesystem UUID: 4696cb59-8675-42e0-a135-5ed08b45ba3d
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000

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

root@archiso ~ #
root@archiso ~ #
root@archiso ~ # mkswap /dev/sda2
Setting up swap space version 1, size = 3.7 GiB (4000313344 bytes)
no label, UUID=3dd6bf5f-49f5-4ce5-80cc-b1c8a07914a8
root@archiso ~ # swapon /dev/sda2
root@archiso ~ # mount /dev/sda1 /mnt
root@archiso ~ # pacstrap /mnt base base-devel gnome vim openssh openvpn rsync bash-completion \
\> traceroute grub sudo wget
```

Рисунок 2 – Загрузка программ для Arch Linux

С помощью команды `genfstab` был создан файл для автоматического монтирования жестких дисков при загрузке в систему.

```
root@archiso ~ # genfstab -U /mnt >> /mnt/etc/fstab
root@archiso ~ # arch-chroot /mnt
[root@archiso /]# ln -sf /usr/share/zoneinfo/Europe/Moscow /etc/localtime
[root@archiso /]# hwclock --systohc
[root@archiso /]# _
```

Рисунок 3 – Создание файла автоматического монтирования жестких дисков

После создания файла монтирования жестких дисков, командой `chroot /mnt`, был осуществлен переход в каталог `/mnt`. Также был установлен загрузчик GRUB и перезагружена система. После перезагрузки был осуществлен переход в сведения о системе (рис. 4). Arch Linux установлен.

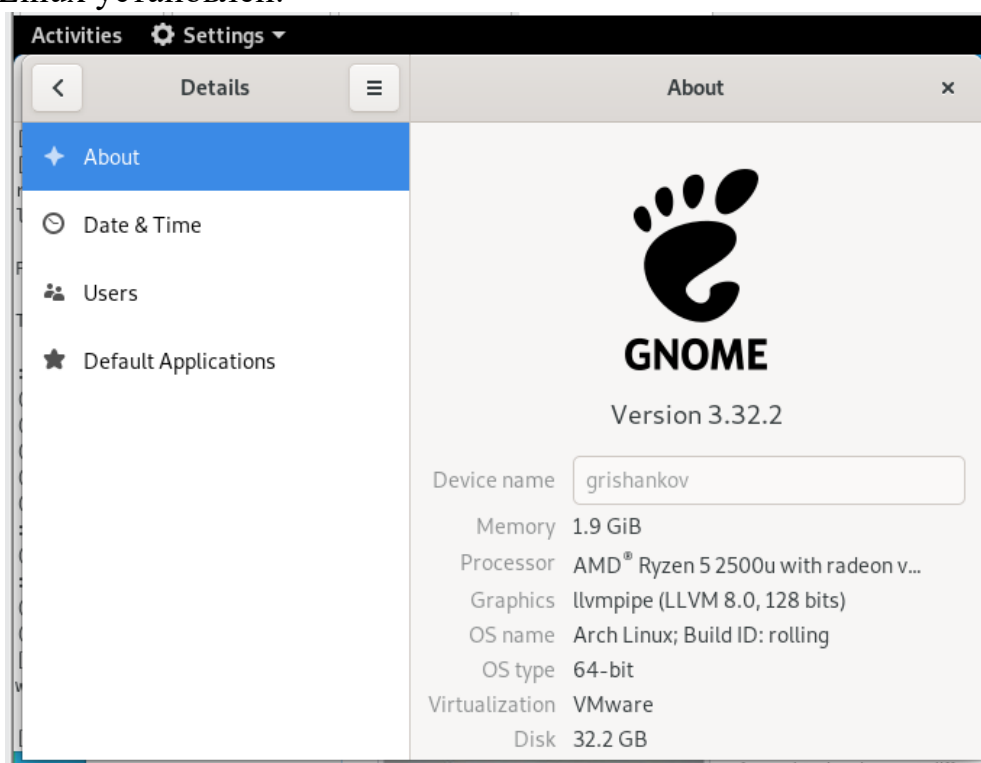


Рисунок 4 – Сведения о системе Arch Linux

1.2 Установка и настройка Samba

Для того чтобы samba сервер принимал сетевой трафик на выделенном сетевом интерфейсе необходимо сначала настроить статический IP адрес и адрес DNS сервера (рис. 5). С помощью командной утилиты nmcli была настроена адресация сетевого адаптера. Ipv4 адрес — 192.168.66.11.[19]



```
[sasha@grishankov ~]$ sudo nmcli connection edit "Wired connection 2"
===| nmcli interactive connection editor |===

Editing existing '802-3-ethernet' connection: 'Wired connection 2'

Type 'help' or '?' for available commands.
Type 'print' to show all the connection properties.
Type 'describe [<setting>.<prop>]' for detailed property description.

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-1x, d
cb, sriov, ethtool, match, ipv4, ipv6, tc, proxy
nmcli> set ipv4.method manual
nmcli> set ipv4.address 192.168.66.11
nmcli> set ipv4.gateway 192.168.66.1
nmcli> set ipv4.dns 127.0.0.1
nmcli> save
Connection 'Wired connection 2' (d02b7e24-a6f0-3a26-8af9-6533cd297c83) successfully u
pdated.
nmcli> quit
```

Рисунок 5 – Настройка IP адресации на сервере Samba

С помощью команды pacman -S --needed были установлены пакеты необходимые для работы с Samba (рис. 6).



```
[sasha@grishankov ~]$ su
Password:
[root@grishankov sasha]# pacman -S --needed samba ntp openresolv bind-tools krb5
```

Рисунок 6 – Установка пакетов с Samba из репозиториев

Командой на рисунке 7 было осуществлено повышение Samba до уровня контроллера домена.[14]

A screenshot of a terminal window with a title bar showing the user 'sasha' at 'grishankov' in the directory '/home/sasha'. The terminal displays a command to provision a Samba domain controller. The command is: `samba-tool domain provision --use-rfc2307 --option="interfaces=lo ens34" --option="bind interfaces only=yes" --server-role=dc --dns-backend=SAMBA_INTERNAL --realm=SMBDC1.SMBDOMAIN.COM --domain=SMBDC1 --adminpass=`. The password field is obscured by a black box. Below the command, a green status line shows: `INFO 2019-05-22 16:33:39.480 pid:1518 /usr/lib/python3.7/site-packages/samba/provisio`.

```
sasha@grishankov:/home/sasha

[root@grishankov sasha]# samba-tool domain provision --use-rfc2307 --option="interfac
es=lo ens34" --option="bind interfaces only=yes" --server-role=dc --dns-backend=SAMBA
_INTERNAL --realm=SMBDC1.SMBDOMAIN.COM --domain=SMBDC1 --adminpass=
INFO 2019-05-22 16:33:39.480 pid:1518 /usr/lib/python3.7/site-packages/samba/provisio
```

Рисунок 7 – повышение Samba до уровня контроллера домена

Были указаны такие сведения как:

- 1) `--use-rfc2307` – использовать UNIX атрибуты для того чтобы пользователи могли использовать учетные записи как для Windows, так и для Linux.
- 2) `--option="interfaces=lo ens34"`, `--option="bind interfaces only"` - принимать запросы от клиентов только на интерфейсах loopback и ens34.
- 3) `--server-role=dc` – сервер будет выступать в качестве контроллера домена
- 4) `--dns-backend=SAMBA_INTERNAL` – в качестве сервера DNS будет использоваться собственное решение от разработчиков проекта Samba.
- 5) `--realm=SMBDC1.SMBDOMAIN.COM` – Область Kerberos (домен, в котором сервер аутентификации Kerberos имеет полномочия для аутентификации пользователей и служб).
- 6) `--domain=SMBDC1` – NetBIOS доменное имя (рабочая группа).
- 7) `--adminpass=*` – пароль администратора

Для того чтобы контроллер домена мог выдавать клиентам настройки времени по протоколу NTP, была произведена конфигурация файла `/etc/ntp.conf` (рис. 8). После сохранения файла необходимо включить демон NTP с помощью команды `systemctl enable ntpd.service`.

```
# Associate to Arch's NTP pool
server 0.arch.pool.ntp.org
server 1.arch.pool.ntp.org
server 2.arch.pool.ntp.org
server 3.arch.pool.ntp.org

# Restrict
restrict default kod limited nomodify nopeer notrap mssntp
restrict 127.0.0.1
restrict ::1
restrict 0.arch.pool.ntp.org mask 255.255.255.255 nomodify notrap nopeer noquery
restrict 1.arch.pool.ntp.org mask 255.255.255.255 nomodify notrap nopeer noquery
restrict 2.arch.pool.ntp.org mask 255.255.255.255 nomodify notrap nopeer noquery
restrict 3.arch.pool.ntp.org mask 255.255.255.255 nomodify notrap nopeer noquery

# Location of drift file
driftfile /var/lib/ntp/ntp.drift

# Location of the update directory
ntpsigndsocket /var/lib/samba/ntp_signd/
~
~
```

Рисунок 8 – Конфигурация NTP на сервере Samba

На рисунке 9 указаны команды которые использовались для конфигурации NTP демона.[8]

```
[root@grishankov sasha]# vim /etc/ntp.conf
[root@grishankov sasha]# sudo mv /etc/ntp.conf{,.default}
[root@grishankov sasha]# sudo cp /etc/ntp.conf.default /etc/ntp.conf
[root@grishankov sasha]# vim /etc/ntp.conf
[root@grishankov sasha]# install -d /var/lib/samba/ntp_signd
[root@grishankov sasha]# chown root.ntp /var/lib/samba/ntp_signd
[root@grishankov sasha]# chmod 0750 /var/lib/samba/ntp_signd
[root@grishankov sasha]# systemctl enable ntpd.service
Created symlink /etc/systemd/system/multi-user.target.wants/ntpd.service → /usr/lib/systemd/system/ntpd.service.
[root@grishankov sasha]#
```

Рисунок 9 – Команды использованные для конфигурации NTP демона

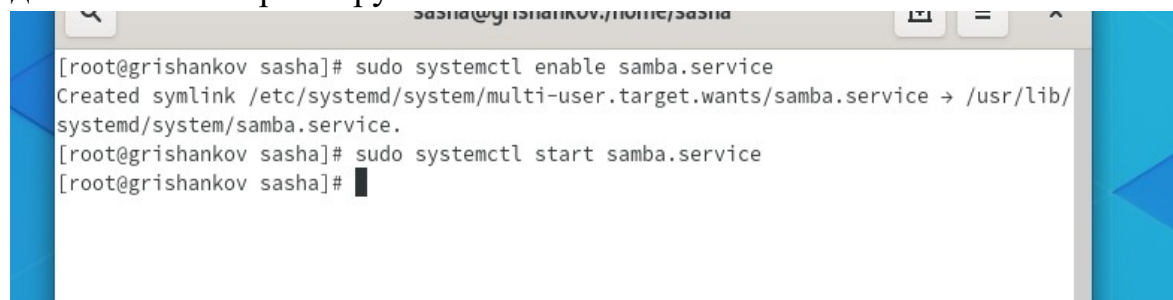
По умолчанию при установке пакета `krb5`, файл с конфигурацией для Kerberos создается автоматически. Необходимо было заменить файл конфигурации Kerberos `/etc/krb5.conf` на файл который был создан при повышении сервера Samba до уровня контроллера домена.

Для того чтобы DNS Server SAMBA_INTERNAL создал запись DNS для компьютера администратора, в файл `/etc/hosts` необходимо добавить запись вида *ip_адрес_компьютера полное_доменное_имя сокращенное_имя*, например:

```
192.168.66.11    grishankov.smbdcl.smbdomain.com grishankov
```

Если необходимо добавить дополнительные DNS серверы в конфигурационный файл `/etc/resolv.conf`, то их следует прописать в файле `/etc/resolv.conf.tail` и выполнить команду `resolvconf -u`.

Samba может функционировать в качестве демона (или в качестве процесса. На рисунке 10 указаны команды для автоматического запуска демона samba при загрузке системы.

A screenshot of a terminal window with a blue title bar. The terminal shows a root user at a machine named 'sasha'. The user enters the command 'sudo systemctl enable samba.service', which results in a message about creating a symlink. Then, the user enters 'sudo systemctl start samba.service', and the prompt returns. The terminal output is as follows:

```
[root@grishankov sasha]# sudo systemctl enable samba.service
Created symlink /etc/systemd/system/multi-user.target.wants/samba.service → /usr/lib/
systemd/system/samba.service.
[root@grishankov sasha]# sudo systemctl start samba.service
[root@grishankov sasha]#
```

Рисунок 10 – Активация демона Samba

После перезагрузки системы был введен ряд команд (рис. 11) для проверки того, что все компоненты samba работают (DNS, Kerberos, LDAP).

```
[root@grishankov sasha]# host -t SRV _ldap._tcp.smbdcl.smbdomain.com
_ldap._tcp.smbdcl.smbdomain.com has SRV record 0 100 389 grishankov.smbdcl.smbdomain.com.
[root@grishankov sasha]# host -t SRV _kerberos._udp.smbdcl.smbdomain.com.
_kerberos._udp.smbdcl.smbdomain.com has SRV record 0 100 88 grishankov.smbdcl.smbdomain.com.
[root@grishankov sasha]# host -t A server.smbdcl.smbdomain.com
Host server.smbdcl.smbdomain.com not found: 3(NXDOMAIN)
[root@grishankov sasha]# host -t A server.smbdcl.smbdomain.com.
Host server.smbdcl.smbdomain.com. not found: 3(NXDOMAIN)
[root@grishankov sasha]# host -t A grishankov.smbdcl.smbdomain.com
grishankov.smbdcl.smbdomain.com has address 192.168.66.11
[root@grishankov sasha]#
```

Рисунок 11 – Проверка работоспособности протоколов DNS, Kerberos, LDAP

Для проверки авторизации было осуществлено подключение к общему ресурсу netlogon, используя учетную запись администратора домена (рис. 12).

```
[root@grishankov sasha]# smbclient //localhost/netlogon -U Administrator -c 'ls'
Enter SMBDC1\Administrator's password:
.          D          0   Wed May 22 16:33:39 2019
..         D          0   Wed May 22 16:33:41 2019

26985432 blocks of size 1024. 19548076 blocks available
[root@grishankov sasha]#
```

Рисунок 12 – Проверка работы netlogon

С помощью команды *kinit* был запрошен Kerberos ticket для учетной записи администратора. Командой *klist* были отображены активные тикеты (рис. 13).

```
[root@grishankov sasha]# kinit administrator@SMBDC1.SMBDOMAIN.COM
Password for administrator@SMBDC1.SMBDOMAIN.COM:
Warning: Your password will expire in 41 days on Wed 03 Jul 2019 04:33:42 PM MSK
[root@grishankov sasha]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@SMBDC1.SMBDOMAIN.COM

Valid starting          Expires                Service principal
05/22/2019 17:29:39    05/23/2019 03:29:39    krbtgt/SMBDC1.SMBDOMAIN.COM@SMBDC1.SMB
DOMAIN.COM
renew until 05/23/2019 17:29:34
```

Рисунок 13 – запрос Kerberos ticket для учетной записи администратора

Командой *samba-tool dns zonecreate* была создана обратная DNS зона для хоста grishankov в домене smbdc1 (рис. 14).

```
[sasha@grishankov ~]$ su
Password:
[root@grishankov sasha]# samba-tool dns zonecreate grishankov.smbdc1.smbdomain.com \
> 66.168.192.in-addr.arpa -U Administrator
Password for [SMBDC1\Administrator]:
Zone 66.168.192.in-addr.arpa created successfully
[root@grishankov sasha]# samba-tool dns add grishankov.smbdc1.smbdomain.com 66.168.192.in-a
ddr.arpa 11 PTR grishankov.smbdc1.smbdomain.com -U Administrator
Password for [SMBDC1\Administrator]:
Record added successfully
[root@grishankov sasha]# systemctl restart samba.service
[root@grishankov sasha]# host -t PTR 192.168.66.11
11.66.168.192.in-addr.arpa domain name pointer grishankov.smbdc1.smbdomain.com.
[root@grishankov sasha]#
```

Рисунок 14 – Создание обратной DNS зоны

Чтобы аутентификация пользователей в домене осуществлялась зашифровано, в главный файл конфигурации Samba `etc/samba/smb.conf` необходимо добавить следующие записи:

```
tls enabled = yes  
tls keyfile = tle/key.pem  
tls certfile = tls/cert.pem  
tls cafile = tls/ca.pem
```

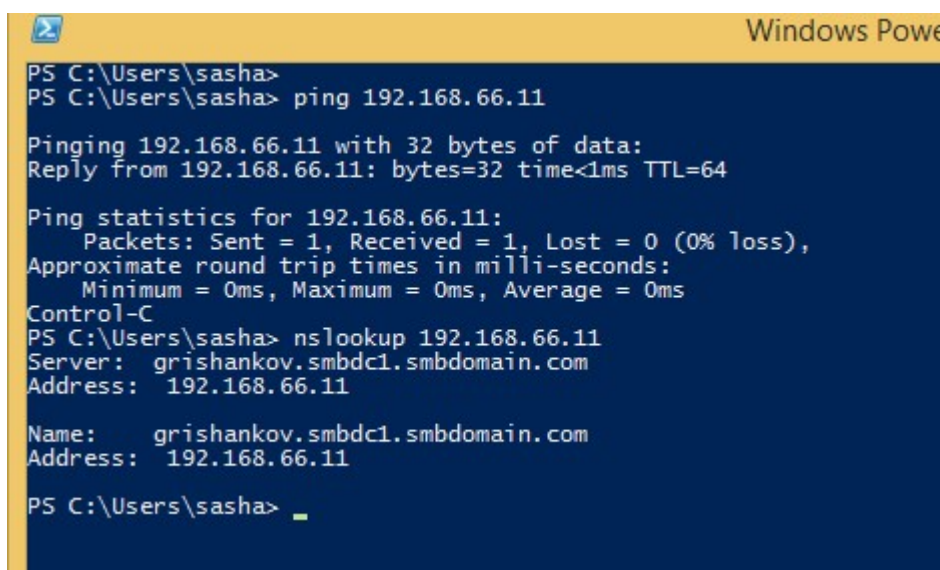
Для проверки поддержки TLS была выполнена команда *smbd -b | grep "ENABLE_GNUTLS"*. В строке вывода должна отображаться запись *ENABLE_GNUTLS*.

ГЛАВА 2 АДМИНИСТРИРОВАНИЕ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ КОМПЬЮТЕРОВ LINUX И WINDOWS

В данной главе клиентские компьютеры на операционных системах Windows и Linux будут введены в домен. Также будут созданы пользователи, настроены и проверены групповые политики пользователей.

2.1 Присоединение компьютера Windows 8.1 к домену

Для машины на базе ОС Windows 8.1 был выбран статический адрес 192.168.66.101. Был указан DNS сервер 192.168.66.11 (Samba сервер). Для того чтобы проверить связь с DNS сервером Samba были выполнены команды ping и nslookup (рис. 15).

A screenshot of a Windows PowerShell terminal window. The title bar is yellow and says "Windows PowerShell". The background is dark blue. The text is white. The user is logged in as "sasha". The commands and their outputs are as follows:

```
PS C:\Users\sasha>
PS C:\Users\sasha> ping 192.168.66.11

Pinging 192.168.66.11 with 32 bytes of data:
Reply from 192.168.66.11: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.66.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\sasha> nslookup 192.168.66.11
Server:  grishankov.smbdc1.smbdomain.com
Address:  192.168.66.11

Name:    grishankov.smbdc1.smbdomain.com
Address:  192.168.66.11

PS C:\Users\sasha> _
```

Рисунок 15 – Проверка связи с DNS сервером

Чтобы в процессе присоединения к домену не возникало ошибок, необходимо настроить правильное время на компьютере Windows. Также следует заранее изменить имя компьютера для удобного администрирования. Было выбрано имя “Win81vm”.

Было указано имя домена smbdc1.smbdomain.com во вкладке “Изменить имя / домен компьютера”.

После нажатия кнопки «ОК» появилось диалоговое окно в котором требуется ввести данные учетной записи администратора домена (рис. 16). В качестве имени используется стандартное имя “Administrator”. В качестве пароля указывается пароль, введенный при повышении Samba до уровня контроллера домена.[15]

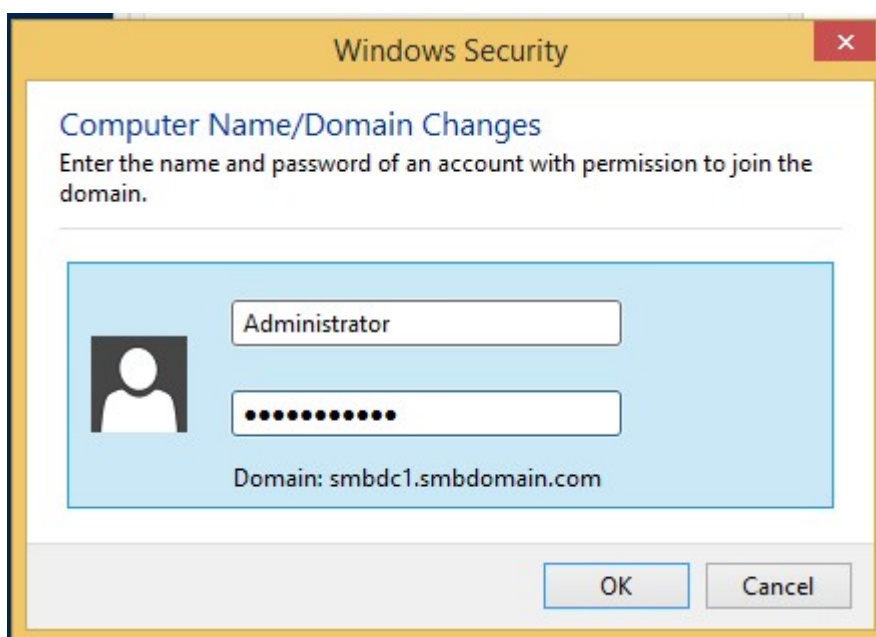


Рисунок 16 – Ввод логина и пароля администратора для ввода компьютера в домен

После нажатия кнопки “ОК” появляется оповещение, которое сообщает, что устройство было введено в домен (рис. 17). Далее необходимо сделать перезагрузку компьютера.

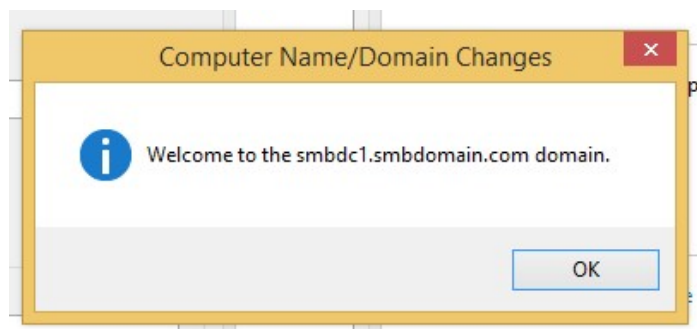


Рисунок 17 – Оповещение об успешном вводе в домен

Вход был осуществлен с учетной записи администратора домена. Во вкладке свойства компьютера видно, что данный компьютер является членом домена smbdc1.smbdomain.com (рис. 18).

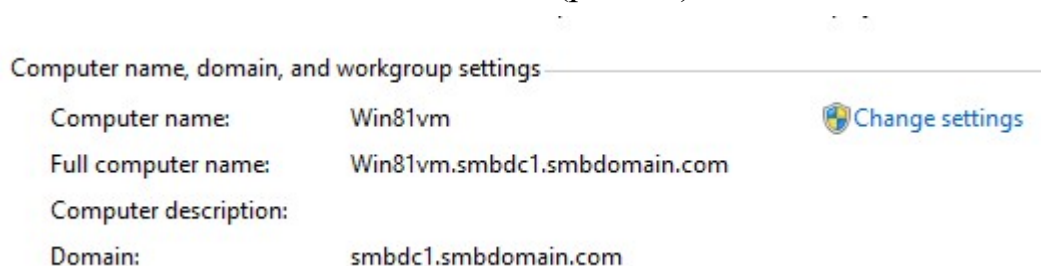
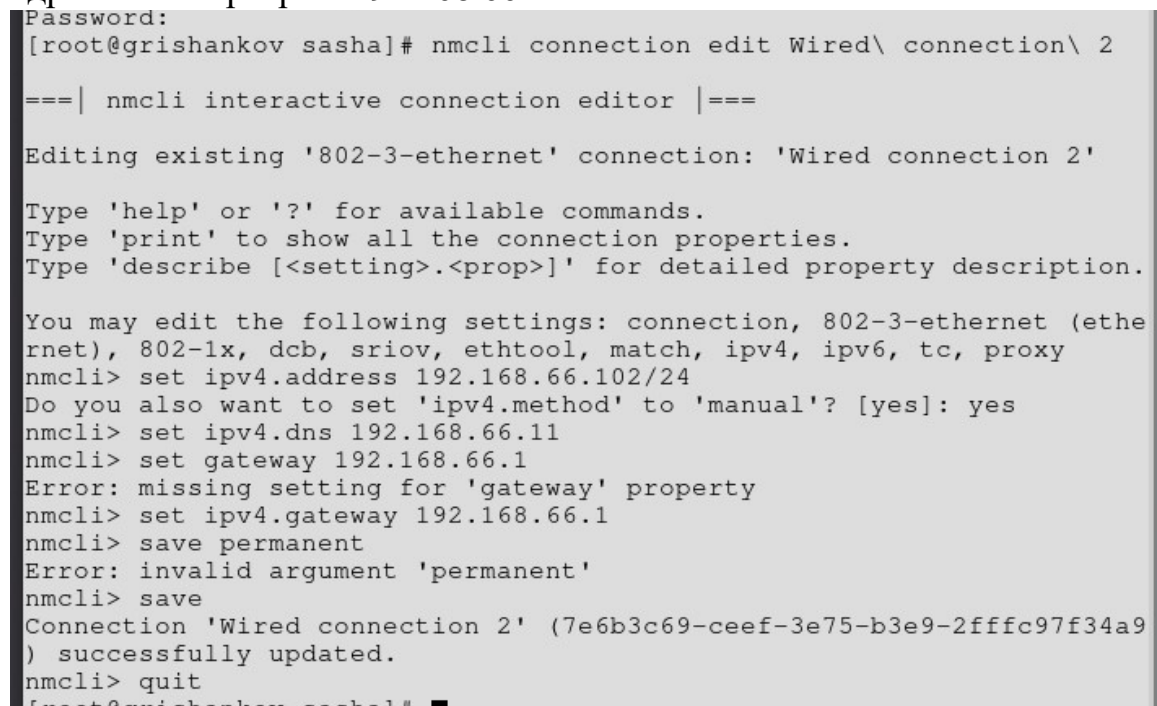


Рисунок 18 – Домен и имя компьютера

2.2 Присоединение компьютера Arch Linux к домену

Для клиентской машины Arch Linux была настроена IP адресация с помощью утилиты nmcli (рис. 19). Адрес клиента — 192.168.66.102/24, адрес DNS сервера – 192.168.66.11.



```

Password:
[root@grishankov sasha]# nmcli connection edit Wired\ connection\ 2
===| nmcli interactive connection editor |===

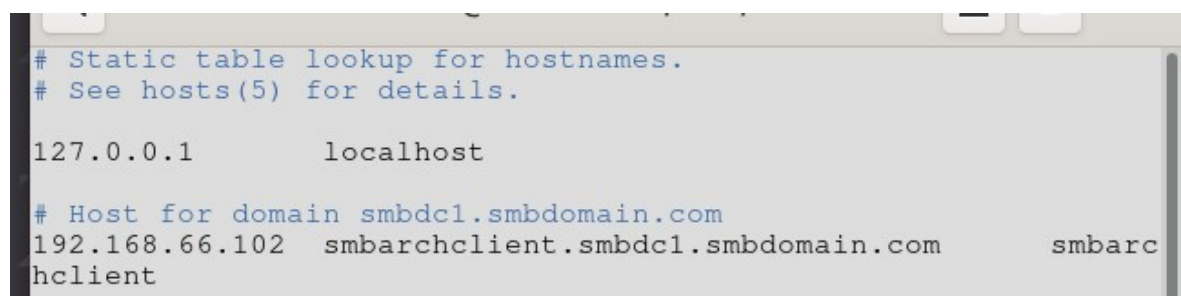
Editing existing '802-3-ethernet' connection: 'Wired connection 2'

Type 'help' or '?' for available commands.
Type 'print' to show all the connection properties.
Type 'describe [<setting>.<prop>]' for detailed property description.

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-lx, dcb, sriov, ethtool, match, ipv4, ipv6, tc, proxy
nmcli> set ipv4.address 192.168.66.102/24
Do you also want to set 'ipv4.method' to 'manual'? [yes]: yes
nmcli> set ipv4.dns 192.168.66.11
nmcli> set gateway 192.168.66.1
Error: missing setting for 'gateway' property
nmcli> set ipv4.gateway 192.168.66.1
nmcli> save permanent
Error: invalid argument 'permanent'
nmcli> save
Connection 'Wired connection 2' (7e6b3c69-ceef-3e75-b3e9-2fffc97f34a9) successfully updated.
nmcli> quit
[root@grishankov sasha]#
```

Рисунок 19 – Настройка IP адресации клиента Linux

Чтобы при присоединении к домену, DNS сервер создал DNS запись для клиента Linux, необходимо ввести IP адрес, короткое, и полное доменное имя (FQDN) данного хоста Linux в файл /etc/hosts (рис. 20).[6]



```

# Static table lookup for hostnames.
# See hosts(5) for details.

127.0.0.1    localhost

# Host for domain smbdc1.smbdomain.com
192.168.66.102  smbarchclient.smbdc1.smbdomain.com  smbarchclient
```

Рисунок 20 – Внесение IP адреса и FQDN клиента Linux в таблицу хостов

С помощью команды *pacman -S --needed bind-tools* был установлен пакет *bind-tools*, который позволяет использовать утилиты *nslookup* для проверки связи с DNS сервером. Связь с DNS сервером Samba была проверена (рис. 21).

```
[root@grishankov sasha]# nslookup
> set type=SRV
> _ldap._tcp.smbdcl.smbdomain.com
Server:      192.168.66.11
Address:     192.168.66.11#53

_ldap._tcp.smbdcl.smbdomain.com service = 0 100 389 grishankov.smbdcl.
smbdomain.com.
> quit
^C
```

Рисунок 21 – Проверка связи с DNS сервером

С помощью команды *pacman -S --needed samba ntp*, была произведена установка пакетов Samba и NTP из репозитория Arch Linux. Конфигурационный файл */etc/ntp.conf* был отредактирован для синхронизации времени с сервером Samba (рис. 22).

```
# Where to retrieve the time from
server DC1.samdom.example.com    iburst prefer

driftfile /var/lib/ntp/ntp.drift
logfile /var/log/ntp

# Access control
# Default restriction: Disallow everything
restrict default ignore

# No restrictions for "localhost"
restrict 127.0.0.1

# Enable the time sources only to only provide time to this host
restrict grishankov.smbdcl.smbdomain.com mask 255.255.255.255 nomo
dify notrap nopeer noquery
```

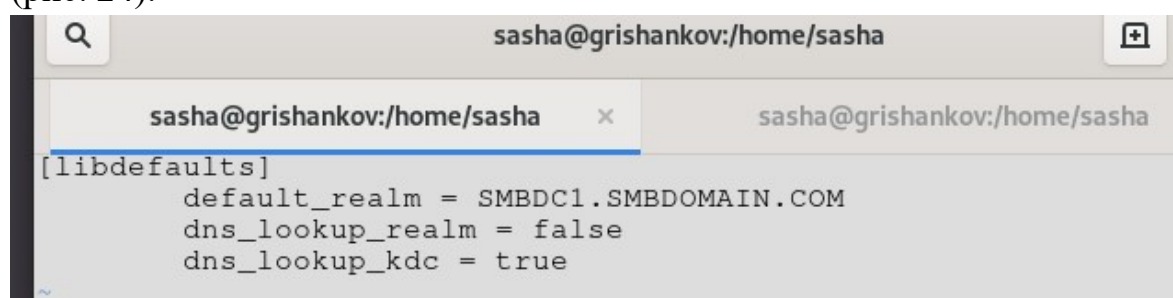
Рисунок 22 – Конфигурация NTP для синхронизации времени с сервером Samba

Демон синхронизации времени был перезагружен. С помощью команды *systemctl status ntpd.service* было проверено что сервис активен (рис. 23).[5]

```
[root@grishankov sasha]# systemctl restart ntpd.service
[root@grishankov sasha]# systemctl status ntpd.service
● ntpd.service - Network Time Service
   Loaded: loaded (/usr/lib/systemd/system/ntpd.service; disabled; ve>
   Active: active (running) since Fri 2019-05-24 12:35:36 MSK; 9s ago
   Process: 5470 ExecStart=/usr/bin/ntpd -g -u ntp:ntp (code=exited, s>
  Main PID: 5472 (ntpd)
     Tasks: 2 (limit: 2343)
    Memory: 1.9M
   CGroup: /system.slice/ntpd.service
           └─5472 /usr/bin/ntpd -g -u ntp:ntp
```

Рисунок 23 – Проверка статуса NTP сервиса

Для того чтобы клиент Linux прошел аутентификацию по протоколу Kerberos необходимо отредактировать файл конфигурации */etc/krb5.conf* и указать доменное имя в верхнем регистре (рис. 24).



```
sasha@grishankov:/home/sasha
[libdefaults]
    default_realm = SMBDC1.SMBDOMAIN.COM
    dns_lookup_realm = false
    dns_lookup_kdc = true
```

Рисунок 24 – Конфигурация аутентификации Kerberos для клиента Linux

Конфигурация для клиента домена Samba производится в файле `/etc/samba/smb.conf`. С помощью параметров на рисунке 25 данный компьютер был сконфигурирован в качестве члена домена `smbdc1.[11]`

```
security = ADS
workgroup = SMBDC1
realm = SMBDC1.SMBDOMAIN.COM

log file = /var/log/samba/%m.log
log level = 1

# Default ID mapping configuration for local BUILTIN accounts
# and groups on a domain member. The default (*) domain:
# - must not overlap with any domain ID mapping configuration!
# - must use a read-write-enabled back end, such as tdb.
idmap config * : backend = tdb
idmap config * : range = 3000-7999
# - You must set a DOMAIN backend configuration
# idmap config for the SAMDOM domain
idmap config SMBDC1:backend = ad
idmap config SMBDC1:schema_mode = rfc2307
idmap config SMBDC1:range = 10000-999999
idmap config SMBDC1:unix_nss_info = yes

vfs objects = acl_xattr
map acl inherit = yes
store dos attributes = yes

# Template settings for login shell and home directory
template shell = /bin/bash
template homedir = /home/%U
```

Рисунок 25 – Конфигурационный файл `smb.conf` для члена домена Samba

Основными параметрами для конфигурации являются:

- 1) *security = ADS* – В этом режиме клиент Samba будет действовать как член домена.
- 2) *workgroup = SMBDC1* – рабочая группа сервера (домен).
- 3) *realm = SMBDC1.SMBDOMAIN.COM* – Kerberos realm. Прописная версия домена AD.

- 4) *idmap config SMBDC1:backend = ad* — использовать LDAP для хранения информации о пользователях Linux и Windows.
- 5) *idmap config SMBDC1:schema_mode = rfc2307* – хранить атрибуты POSIX для возможности использования учетных записей как на Windows так и на Linux.
- 6) *idmap config SMBDC1:range = 10000-999999* – числовой лимит идентификаторов для пользователей, групп и компьютеров домена.
- 7) *idmap config SMBDC1:unix_nss_info = yes* – хранить атрибуты POSIX для возможности использования разных командных оболочек и домашних каталогов пользователями Linux.

Для ввода компьютера Linux в домен была использована команда *net ads join -U administrator* с указанием пароля администратора домена. Командная строка отображает что хост SMBARCHCLIENT был присоединен к домену smbdc1 (рис. 26).[16]



```
sasha@smbarchclient:/home/sasha
[root@smbarchclient sasha]#
[root@smbarchclient sasha]# net ads join -U administrator
Enter administrator's password:
Using short domain name -- SMBDC1
Joined 'SMBARCHCLIENT' to dns domain 'smbdc1.smbdomain.com'
[root@smbarchclient sasha]#
```

Рисунок 26 – Хост smbarchclient присоединен к домену.

2.3 Создание и аутентификация пользователей домена, общий доступ к файлам и папкам.

Необходимо осуществить вход в Windows от имени администратора домена (рис. 27).

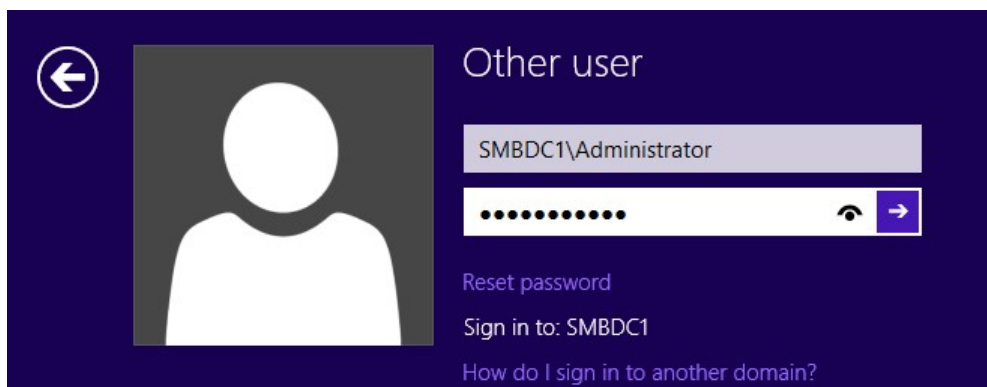


Рисунок 27 – Вход в систему от имени администратора домена

С официального сайта Microsoft была произведена загрузка средств для удаленного администрирования сервера (RSAT). Данное программное обеспечение бесплатно предоставляется компанией Microsoft для всех версий клиентских компьютеров семейства Windows. После установки RSAT, был открыт менеджер серверов.[18] Добавление контроллера домена Samba в список серверов осуществляется вручную. Samba DC был добавлен в список серверов с помощью инструмента RSAT “добавить сервер” (рис. 28).

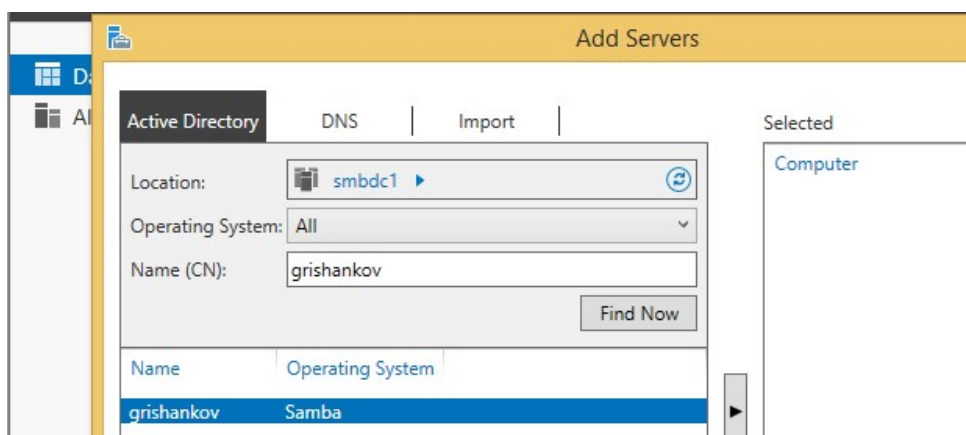


Рисунок 28 – Добавление Samba DC в список серверов

Чтобы осуществлять управление учетными записями пользователей для машин Linux был включен режим расширенных возможностей в окне пользователи и компьютеры Active Directory (рис. 29).[7]

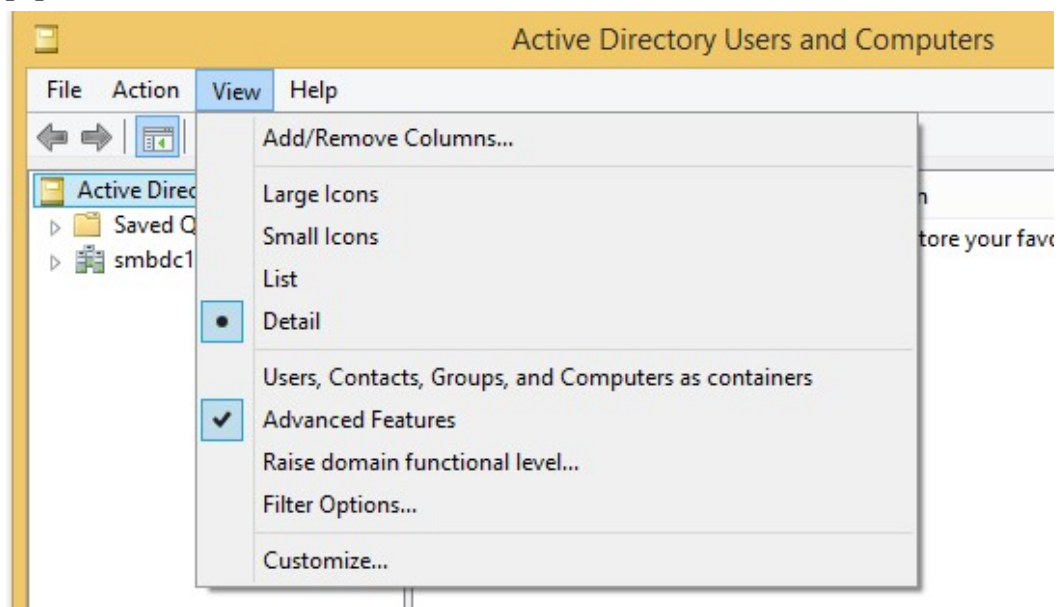


Рисунок 29 – Включение расширенных возможностей для пользователей и компьютеров Active Directory

Чтобы заходить на компьютеры Linux от имени администратора домена (или других пользователей), необходимо открыть свойства пользователя Administrator с помощью инструмента “пользователи и компьютеры Active Directory”, открыть панель “атрибуты Unix” (рис. 30) и заполнить поля:

- 1) *NIS Domain* (имя домена для пользователей Linux), *UID* (ID пользователя для Linux)
- 2) *Login Shell* (командная оболочка)

- 3) *Home Directory* (домашний каталог пользователя)
- 4) *Primary Group* (основная группа для пользователей Linux)

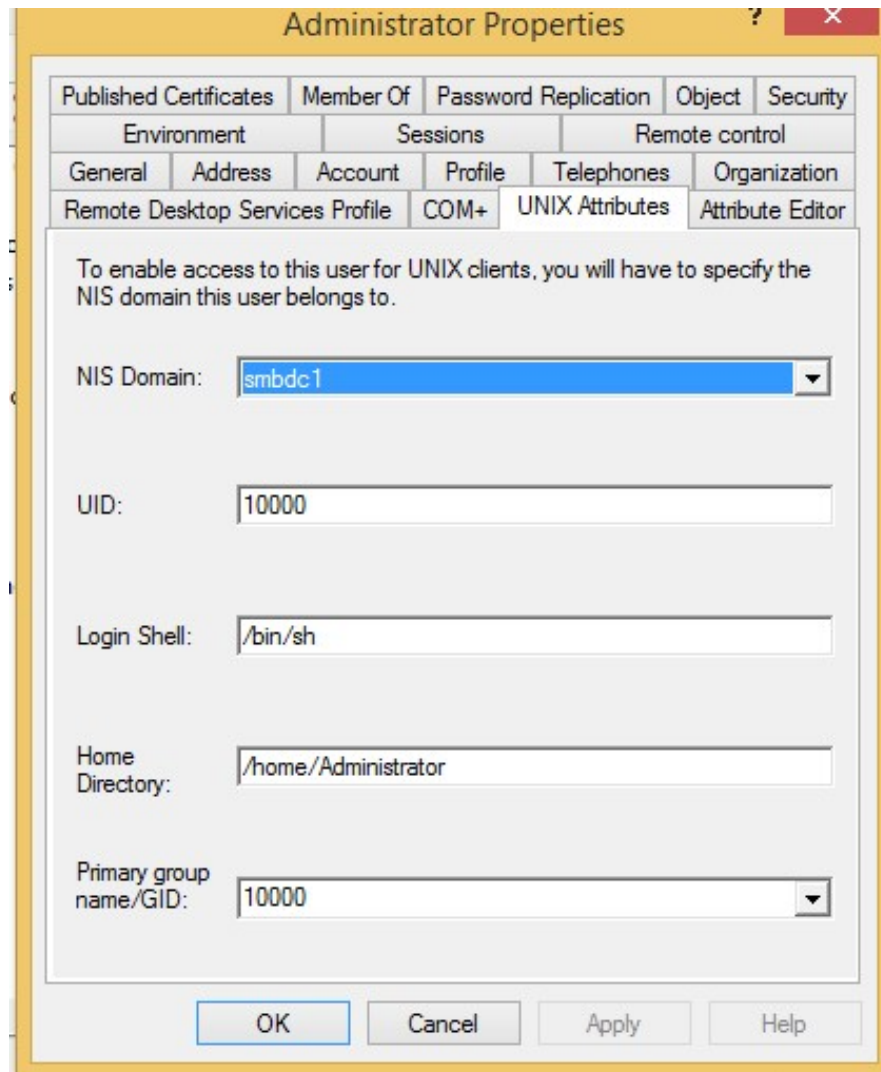


Рисунок 30 – Редактирование атрибутов Unix для пользователя Administrator

Любой пользователь Linux в домене должен иметь информацию о первичной группе (GID), иначе вход в домен будет невозможен . Для этого необходимо присвоить UNIX атрибут *GID (Group ID)* с помощью Windows RSAT или с помощью samba-tool на сервере Samba DC.

Так как любому пользователю домена автоматически присваивается группа “Domain Users” в качестве первичной, данной группе был присвоен GID 10001 (рис. 31).

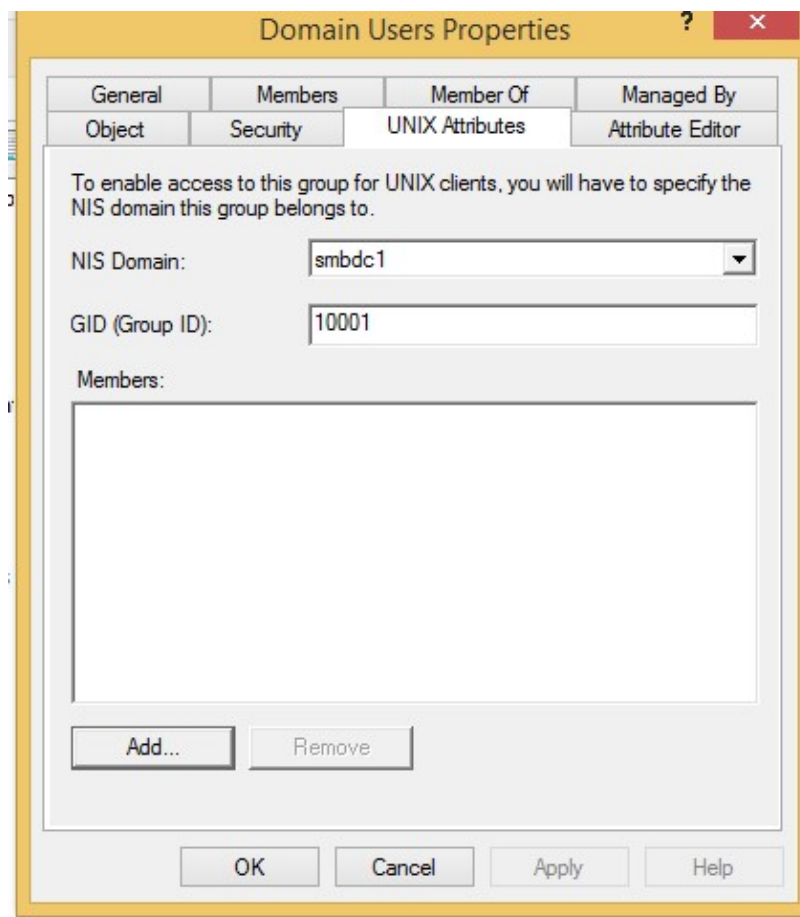


Рисунок 31 – Редактирование атрибута Unix GID для группы Domain Users

Компьютеры Linux будут иметь доступ к общим файлам и папкам компьютеров Windows при условии, что будет настроен Unix атрибут uidNumber во вкладке “Attribute Editor” в свойствах компьютера AD. uidNumber должен быть уникален для каждого компьютера.

На рисунке 32 отображена настройка uidNumber для компьютера Win81vm.

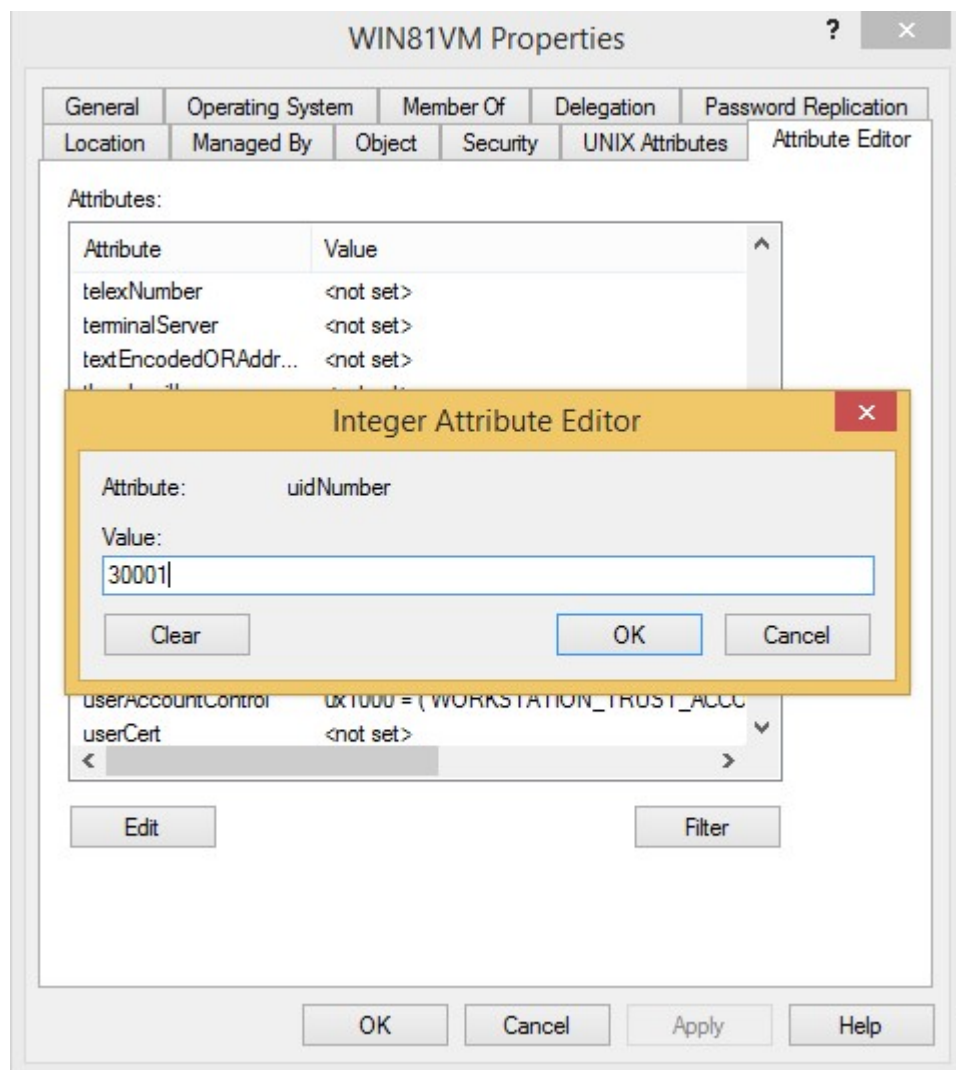


Рисунок 32 – Настройка атрибута uidNumber для компьютера Win81vm

С помощью командной утилиты для администрирования пользователей "samba-tool" был создан пользователь gpouser2.

Утилита позволяет сразу ввести Unix атрибуты (рис. 33).[9]

```
[root@grishankov sasha]#  
[root@grishankov sasha]# samba-tool user create gpouser2 Gpouser020497 --unix-home=/home/gpouser2 --uid-number=10101 --login-shell=/bin/bash --gid-number=10100 --nis-domain=smbdc1  
User 'gpouser2' created successfully  
[root@grishankov sasha]#
```

Рисунок 33 – Создание пользователя домена gpouser2 с помощью утилиты samba-tool

Аутентификация пользователя домена gpouser2 была проверена на операционной системе Windows. Для этого были введены учетные данные smbdc1\gpouser2 (домен\пользователь) и пароль пользователя (рис. 34).

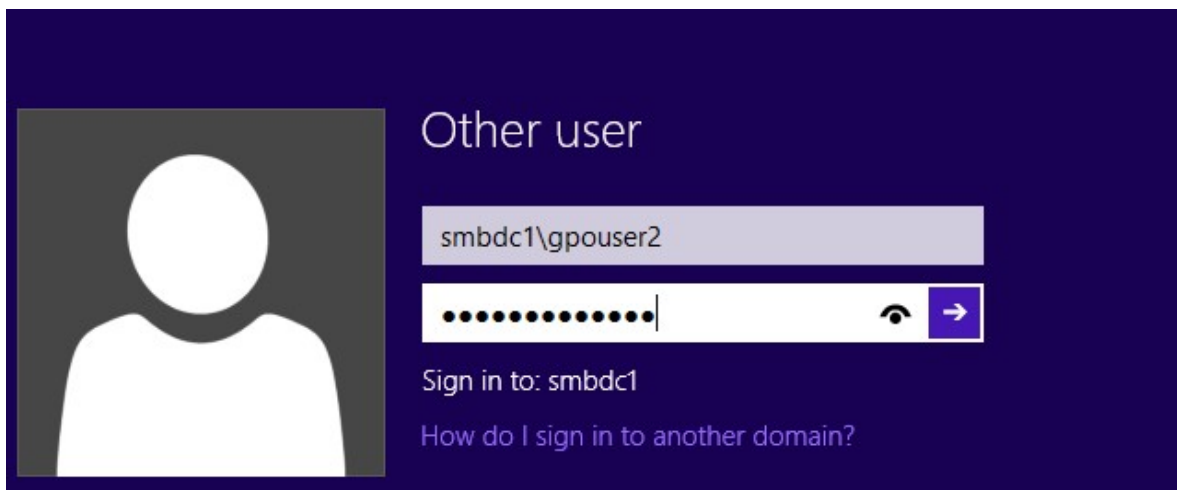


Рисунок 34 – Аутентификация пользователя gpouser2 на ОС Windows

На рисунке 35 показано, что пользователь успешно прошел аутентификацию на компьютере Windows.



Рисунок 35 – Пользователь gprouser2 аутентифицирован

Для разрешения имен пользователей учетных записей домена с помощью winbind, на клиентском компьютере Linux “smbarchclient” необходимо отредактировать файл /etc/nsswitch.conf как показано на рисунке 36.[12]

```
# Name Service Switch configuration file.
# See nsswitch.conf(5) for details.

passwd: files winbind mymachines systemd
group: files winbind mymachines systemd
shadow: files
```

Рисунок 36 – Конфигурация файла nsswitch.conf для разрешения имен пользователей домена

Далее следует выполнить команды *smbd*; *nmdb*; *winbindd* для запуска основных процессов Samba на клиентском компьютере Linux.

Аутентификация пользователей домена на компьютерах Linux требует конфигурации подключаемых модулей аутентификации (PAM) на использование модулей “pam_winbind.so”.[13] Конфигурационный файл для аутентификации пользователей находится в каталоге /etc/pam.d/system-auth. Полная конфигурация данного файла показана на рисунке 37.[10]

```
##PAM-1.0

auth    sufficient pam_winbind.so
auth    required  pam_unix.so      try_first_pass nullok
auth    optional  pam_permit.so
auth    required  pam_env.so

account sufficient pam_winbind.so
account required  pam_unix.so
account optional  pam_permit.so
account required  pam_time.so

password required  pam_unix.so      try_first_pass nullok sha512 shadow
password optional  pam_permit.so

session required  pam_limits.so
session required  pam_unix.so
session optional  pam_permit.so

~
~
~
~
```

Рисунок 37 – Конфигурация подключаемых модулей аутентификации (PAM)

Необходимо создать домашние каталоги для пользователей домена. Для каждого созданного домашнего каталога был указан владелец (пользователь домена) и его группа (рис. 38).

Если домашний каталог пользователя будет отсутствовать, то он не сможет осуществить вход в графическую оболочку GNOME будет НЕВОЗМОЖЕН.

```
[sasha@smbarchclient ~]$ su
Password:
[root@smbarchclient sasha]# mkdir /home/Administrator
[root@smbarchclient sasha]# mkdir /home/gpouser2
[root@smbarchclient sasha]# chown -R "SMBDC1\Administrator:SMBDC1\domain users"
/home/Administrator
[root@smbarchclient sasha]# chown -R "SMBDC1\gpouser2:SMBDC1\gpogroup" /home/gpo
user2
[root@smbarchclient sasha]#
```

Рисунок 38 – Создание домашних каталогов на компьютере Linux для пользователей домена

После перезагрузки системы в окне менеджера дисплеев Gnome (gdm) были введены данные учетной записи администратора домена (рис. 39).

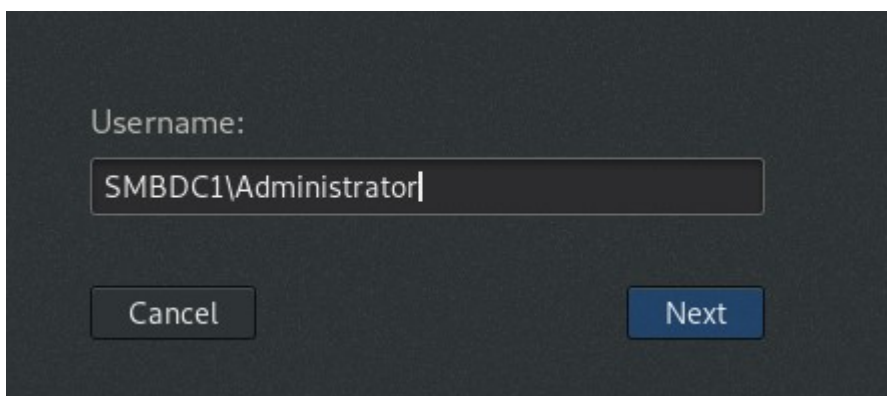


Рисунок 39 – Ввод данных учетной записи администратора домена в окне gdm

Вход в учетную запись администратора домена был выполнен. Для того, чтобы проверить, что на данный момент используется учетная запись администратора домена была открыта панель “пользователи” в настройках системы (рис. 40).

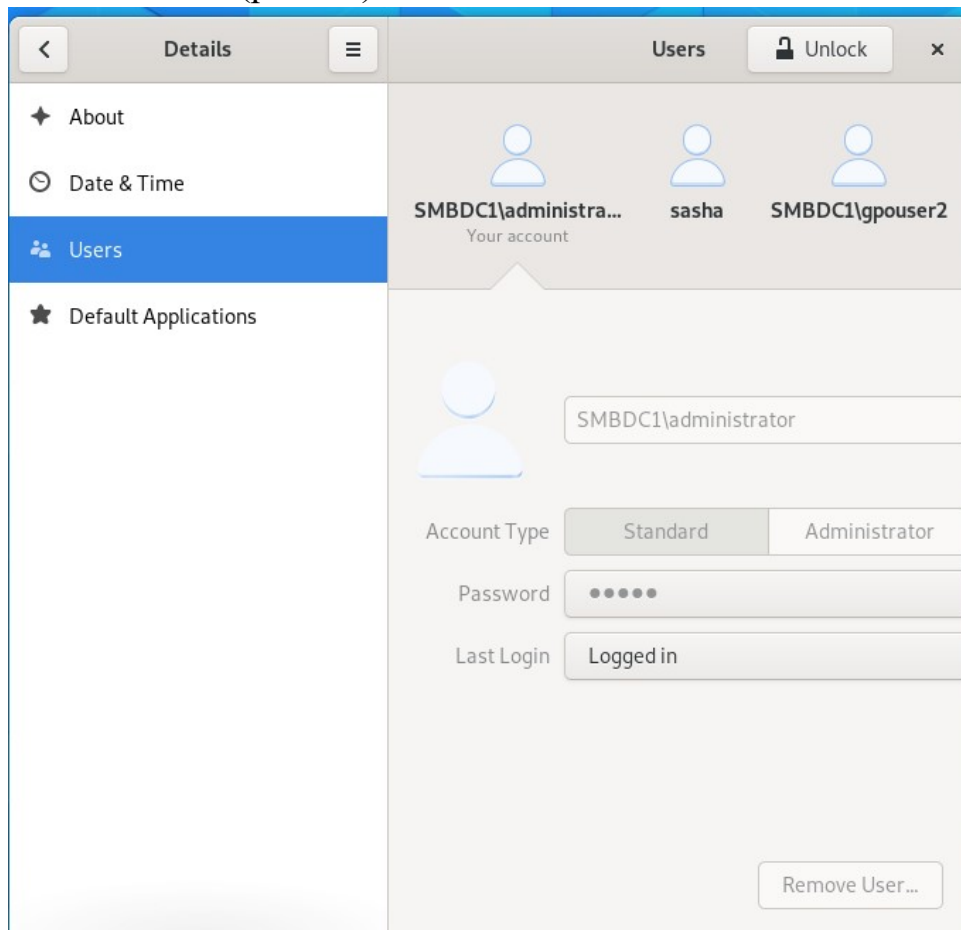


Рисунок 40 – Проверка имени пользователя системы

Для общего доступа к папке, необходимо ее создать, присвоить права и указать доменную группу в качестве владельца (рис. 41).

```
[root@smbarchclient sasha]# mkdir -p /srv/samba/Demo/
[root@smbarchclient sasha]# chmod 2770 /srv/samba/Demo/
[root@smbarchclient sasha]# chown root:gpogroup /srv/samba/Demo/
chown: invalid group: 'root:gpogroup'
[root@smbarchclient sasha]# chown root:SMBDC1\gpogroup /srv/samba/Demo/
[root@smbarchclient sasha]#
```

Рисунок 41 — Создание общего доступа к папки “Demo”

В конфигурационном файле Samba для члена домена необходимо указать на данную общую папку с помощью строк на рисунке 41.

```
[global]
    acl allow execute always = yes
[Demo]
    path = /srv/samba/Demo/
    read only = no
```

Рисунок 42 — Параметры конфигурационного файла Samba для создания общей папки Demo

Был осуществлен вход в домен от имени пользователя gpouser1. После чего было проверено, что пользователь обладает правами для создания файла в общей папки (рис. 42).

```
[SMBDC1\gpouser1@smbarchclient ~]$ cd /srv/samba/Demo/
[SMBDC1\gpouser1@smbarchclient Demo]$ rm -r gpouser1
[SMBDC1\gpouser1@smbarchclient Demo]$ touch file.txt
[SMBDC1\gpouser1@smbarchclient Demo]$ echo hello world >> file.txt
[SMBDC1\gpouser1@smbarchclient Demo]$
```

Рисунок 43 — Создание файла в общей папки

Был осуществлен вход в домен от имени пользователя gpouser2. Пользователь смог прочитать содержимое файла, созданного пользователем gpouser1 (рис. 43).

```
[SMBDC1\gpouser2@smbarchclient ~]$ cd /srv/samba/Demo/
[SMBDC1\gpouser2@smbarchclient Demo]$ cat file.txt
hello world
[SMBDC1\gpouser2@smbarchclient Demo]$
```

Рисунок 44 — Чтение содержимого общей папки