

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования



НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

ОТЧЕТ

по лабораторной работе №1

«Сетевое взаимодействие Windows и Linux»

по дисциплине

«Администрирование систем и сетей»

РУКОВОДИТЕЛЬ:

(подпись)

Кочешков А. А.

(фамилия, и.,о.)

СТУДЕНТ:

(подпись)

Сухоруков В.А.

(фамилия, и.,о.)

19-ВМ

(шифр группы)

Работа защищена «__» _____

С оценкой _____

Нижний Новгород 2023

Оглавление

Цель работы	4
Ход работы.....	4
Часть 1. Взаимодействие на базе протокола SMB.	4
1. Проверка сетевого доступа по протоколу TCP/IP	4
1.1. Получить информацию по настройке сетевых интерфейсов. Сконфигурировать стек по минимальным параметрам.	4
1.2. Настроить локальные файлы трансляции DNS-имен.	5
2. Реализация сервера файлового доступа SMB на Linux-системе.....	7
2.1. Ознакомиться с составом Samba.....	7
2.2. Изучить конфигурирование Samba.	8
2.3. Создать учетную запись пользователя Samba.....	9
2.4. Внутри локального каталога /pub сформировать каталог для выделения в сетевой доступ по smb протоколу.....	10
2.5. Подготовить условия для подключения smb-клиентов и стартовать сервер Samba.	11
2.6. В Windows-клиенте проверить доступность и свойства сетевых ресурсов.	11
2.7. Схема сетевого взаимодействия (SMB, Клиент –Windows, Сервер - Linux)	16
3. Работа SMB-клиента в Linux	17
3.1. Использование команды smbclient	17
3.2. Использование команды smbtree	18
3.3. Использование команды mount.cifs.....	19
3.4. Использование команды smbstatus	20
3.5. Схема сетевого взаимодействия (SMB, Клиент –Linux, Сервер - Linux)	21
4. Использование команды net.	21
2 Часть. Взаимодействие на базе протокола NFS	22
5. Сетевая файловая система NFS в Linux.	22
5.1. Найти основные компоненты, необходимые для работы NFS	22
5.2. Выделение каталога в общий доступ	23
5.3. Запуск NFS.....	24
5.4. Монтирование сетевой файловой системы	25
5.5. Схема сетевого взаимодействия (NFS, Клиент –Linux, Сервер - Linux)	25
6. Использование в Windows Server служб Service for NFS для организации сетевого доступа по протоколу NFS.	26
6.1. Настроить файл-сервер в Windows Server	26
6.2. Рассмотреть средства согласования учетных записей и свойства службы отображения имен.	26
6.3. Служба «Сервер для NFS»	28
6.4. На Windows-сервере создать каталог, определить разрешения доступа NTFS. Средствами эксплорера в свойствах каталога настроить параметры экспорта каталога по NFS.....	29

6.5. На Windows-сервере с помощью консоли администрирования перезапустить сервер NFS. Командой showmount отобразить состояние ресурсов NFS.	29
6.6. Схема сетевого взаимодействия (NFS, Клиент –Linux, Сервер – Windows, сопоставленный доступ)	30
6.7. Схема сетевого взаимодействия (NFS, Клиент –Linux, Сервер – Windows, не сопоставленный доступ)	32
7. Использование NFS-клиента на Windows Server.	33
7.1. Рассмотреть свойства службы “Клиент для NFS”. Стартовать службу.	33
7.2. Применить NFS-клиент на Windows для монтирования ресурса на NFS-сервере Linux.....	33
7.3. Схема сетевого взаимодействия (NFS, Клиент –Windows, Сервер – Linux).....	34
Вывод.....	34

Цель работы

Изучение механизмов и средств интеграции Windows и Linux на базе сетевых файловых систем.

Ход работы

Часть 1. Взаимодействие на базе протокола SMB.

1. Проверка сетевого доступа по протоколу TCP/IP

1.1. Получить информацию по настройке сетевых интерфейсов. Сконфигурировать стек по минимальным параметрам.

Для соединения двух виртуальных машин в одну сеть установим в свойствах виртуальных машин тип подключения «Сетевой мост». С помощью команд `ifconfig` для ОС Astra Linux, и `ipconfig` для ОС Windows 7 получим информацию о настройке сети.

```
valerii@ValeriiAstra:~$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.108 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::ec7:255e:8bb3:f3c8 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:29:ff:90 txqueuelen 1000 (Ethernet)
    RX packets 1935 bytes 190458 (185.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 161 bytes 15099 (14.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рис 1.

```
C:\Users\valerii>ipconfig

Настройка протокола IP для Windows

Ethernet adapter Подключение по локальной сети:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::918f:59bf:9f68:f823%11
    IPv4-адрес . . . . . : 192.168.0.103
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . : 192.168.0.1
```

Рис 2.

- ❖ IP адреса были получены от DHCP сервера.
- ❖ Машины находятся в сети 192.168.0.0 с маской сети 255.255.255.0,
- ❖ Адрес машины Valerii-Win7 192.168.0.103,
- ❖ Адрес машины ValeriiAstra 192.168.0.108

Настроим статические IP адреса на обеих машинах. В свойствах сети на машине ValeriiAstra изменим метод получения IP адреса с «Автоматический (DHCP)» на «Вручную», и установим нужные параметры.

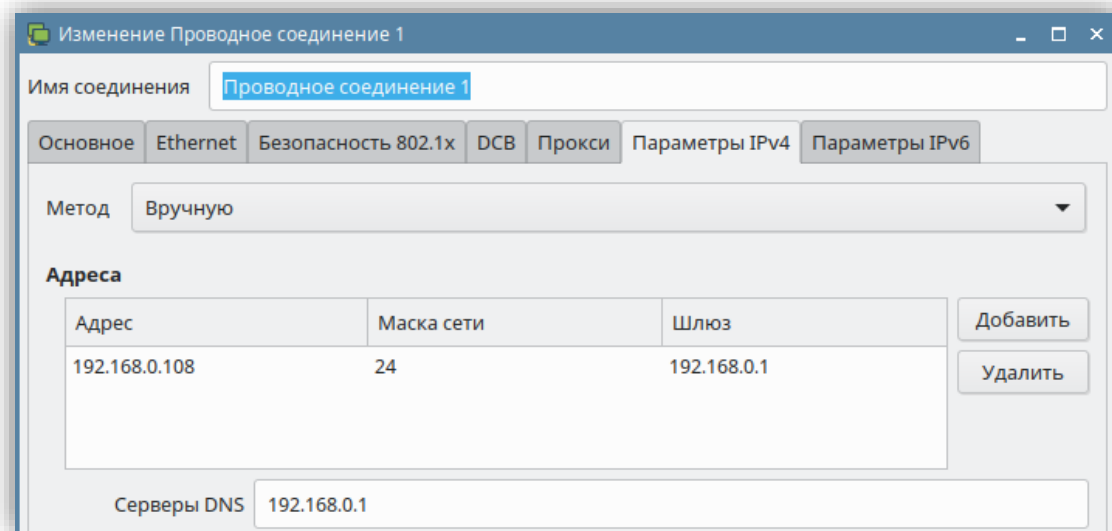


Рис 3.

Также настроим сеть на узле Windows.

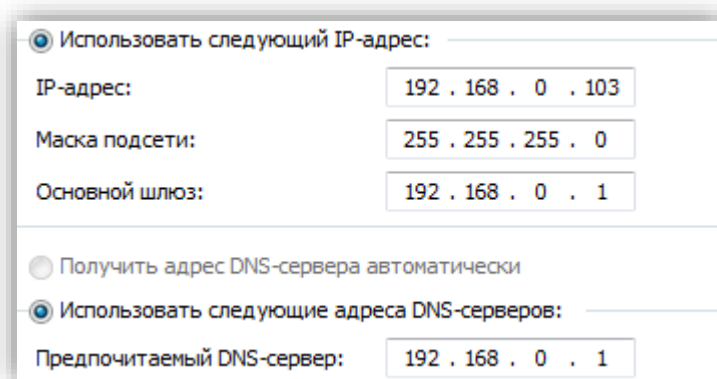


Рис 4.

Проверим доступность сети командой ping.

```
valerii@ValeriiAstra:~$ ping 192.168.0.103
PING 192.168.0.103 (192.168.0.103) 56(84) bytes of data:
64 bytes from 192.168.0.103: icmp_seq=1 ttl=128 time=0.313 ms
64 bytes from 192.168.0.103: icmp_seq=2 ttl=128 time=0.243 ms
64 bytes from 192.168.0.103: icmp_seq=3 ttl=128 time=0.293 ms
```

Рис 5.

Сеть доступна, и работает корректно.

1.2. Настроить локальные файлы трансляции DNS-имен.

Произведём настройку на узле Linux. Внесем изменения в файл **/etc/hosts**, который содержит информацию о соответствии DNS имен сетевым адресам. Добавим строку с адресом и именем узла Windows.

```
/etc/hosts [-M--] 28 L: [
127.0.0.1<----->localhost
127.0.1.1<----->ValeriiAstra
192.168.0.103<->Valerii-Win7
```

Рис 6.

Файл /etc/samba/lmhosts, который содержит информацию о соответствии NetBIOS имен сетевым адресам. В текущей версии системы данный файл отсутствует. Создадим его, и добавим строки с адреса и именами узлов Windows и Linux.

```
/etc/samba/lmhosts [----] 28
192.168.0.103<->Valerii-Win7
192.168.0.108<->ValeriiAstra
127.0.1.1<----->ValeriiAstra
```

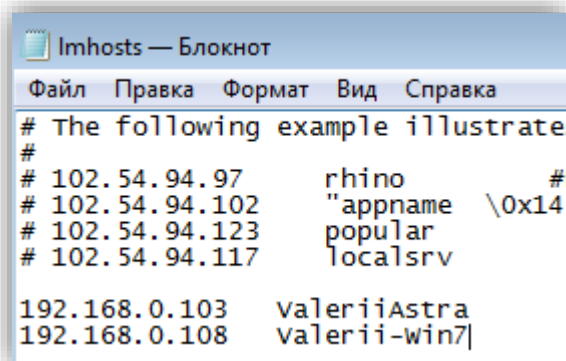
Рис 7.

Произведём настройку на узле Windows. В файл %SYSTEMROOT%\system32\drivers\etc\hosts запишем соответствие DNS имени и ip-адреса хоста на Linux машине.

```
# For example:
#
#      102.54.94.97      rhino.acme.com
#      38.25.63.10      x.acme.com
#      192.168.0.108    ValeriiAstra
```

Рис 8.

В файл %SYSTEMROOT%\system32\drivers\etc\lmhosts.asm запишем соответствие NetBIOS имени и ip-адреса хоста на Linux и Windows машинах.



```
lmhosts — Блокнот
Файл  Правка  Формат  Вид  Справка
# The following example illustrate
#
# 102.54.94.97      rhino      #
# 102.54.94.102     "appname  \0x14
# 102.54.94.123     popular
# 102.54.94.117     localsrv

192.168.0.103      valeriiAstra
192.168.0.108      valerii-win7
```

Рис 9.

Проверим доступность узлов указав в команде ping DNS адреса узлов.

```
C:\Users\valerii>ping ValeriiAstra

Обмен пакетами с ValeriiAstra [192.168.0.108] с 32 байтами данных:
Ответ от 192.168.0.108: число байт=32 время<1мс TTL=64
Ответ от 192.168.0.108: число байт=32 время<1мс TTL=64
Ответ от 192.168.0.108: число байт=32 время<1мс TTL=64
Ответ от 192.168.0.108: число байт=32 время<1мс TTL=64
```

Рис 10.

```

valerii@ValeriiAstra:~$ ping Valerii-Win7
PING Valerii-Win7 (192.168.0.103) 56(84) bytes of data:
64 bytes from Valerii-Win7 (192.168.0.103): icmp_seq=1 ttl=128 time=0.258 ms
64 bytes from Valerii-Win7 (192.168.0.103): icmp_seq=2 ttl=128 time=0.252 ms
64 bytes from Valerii-Win7 (192.168.0.103): icmp_seq=3 ttl=128 time=0.186 ms
64 bytes from Valerii-Win7 (192.168.0.103): icmp_seq=4 ttl=128 time=0.244 ms
^C
--- Valerii-Win7 ping statistics ---

```

Рис 11.

Доступ по сети через DNS адреса возможен. Сеть настроена корректно.

2. Реализация сервера файлового доступа SMB на Linux-системе.

2.1. Ознакомиться с составом Samba.

Samba- пакет программ, который позволяет обращаться к сетевым дискам на различных операционных системах по протоколу SMB. Имеет клиентскую и серверную части и является свободным программным обеспечением.

Для установки samba выполним команду **sudo apt-get install samba**

```

valerii@ValeriiAstra:~$ sudo apt-get install samba
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Уже установлен пакет samba самой новой версии (2:4.9.5+dfsg-5+deb10u3astra.ce1),
обновлено 0, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов
не обновлено.
valerii@ValeriiAstra:~$ █

```

Рис 12.

Самая последняя версия уже установлена. Ознакомимся с составом samba.

/etc/samba/...

- ❖ lmhosts - файл соответствия NetBIOS- имен и IP- адресов
- ❖ smb.conf- основной конфигурационный файл свойств сервера и описания сетевых ресурсов

< /etc/samba .[^]>			
.u	Имя	Размер	Время правки
/..		-ВВЕРХ-	мар 6 11:12
/tls		4096	июн 10 2022
gdbcommands		8	июн 10 2022
lmhosts		76	мар 6 11:24
smb.conf		8629	фев 7 12:47

Рис 13.

/usr/sbin/...

- ❖ smbd- демон SMB-сервера. Обрабатывает соединение с клиентом, проверяет полномочия клиента и может сам аутентифицировать пользователя, реализует доступ клиента к сетевым ресурсам
- ❖ nmbd- сервер имен NetBIOS. Выполняет функции сетевого браузера для механизма обзора сети, может выполнять функции клиента и сервера WINS, а также WINS-проху

- ❖ winbindd- демон аутентификации в домене Active Directory по протоколу Kerberos
- ❖ mount.cifs- утилита монтирования smb-ресурса к локальной файловой системе для последующей более легкой работы с удаленными файлами как с локальными

*smbd	84064	июн 10 2022
*nmbd	247832	июн 10 2022

Демон winbindd и утилита mount.cifs отсутствуют в данной версии.

/usr/bin/...

- ❖ pdbedit- редактор учетных записей в базе tdb, ldap
- ❖ testparm- утилита тестирования правильности параметров в конфигурации smb.conf
- ❖ smbpasswd- утилита управления пользователями Samba
- ❖ smbstatus- отображает текущее состояние smb-сеансов
- ❖ smbclient- клиентская программа доступа к smb-ресурсам в формате командной среды
- ❖ smbtree- smb-обозреватель в текстовом режиме
- ❖ net- утилита удаленного администрирования smb- серверов с использованием трех вариантов протоколов: ADS, RPC, RAP

*pdbedit	40648	июн 10 2022
*testparm	30712	июн 10 2022
*smbpasswd	30712	июн 10 2022
*smbstatus	30720	июн 10 2022
*smbtree	14336	июн 10 2022
*net	880936	июн 10 2022

2.2. Изучить конфигурирование Samba.

Для работы Samba необходим файл **smb.conf**- конфигурационный файл, который структурирован по разделам с указанием названия одной из трех секций:

- ❖ [homes] - позволяет настроить доступ к домашней директории пользователя.
- ❖ [printers] – раздел принтеров, который задает общие правила использования принтеров Linux, описанных в файле /etc/printcap
- ❖ [global] – определяет переменные, которые Samba будет использовать для определения доступа ко всем ресурсам.

Установим необходимые параметры конфигурационного файла smb.conf:

- ❖ workgroup - Определяет, в какой рабочей группе будет находиться сервер.
- ❖ NetBIOS name - Устанавливает NetBIOS-имя Samba-сервера. По умолчанию оно совпадает с первым компонентом DNS-имени хоста.
- ❖ security- определяет режим безопасности в соответствии с механизмом аутентификации SMB. Режим доступа на уровне пользователя подразумевает аутентификацию либо самим сервером Samba по своей базе учетных записей, либо на каком- либо внешнем сервере аутентификации.

Установим Режим безопасности на уровне пользователей с аутентификацией по БД УЗ Samba в формате tdb:

```
security = user
passdb backend = tdbsam
```

Разрешим использовать версию протокола SMB1.


```

/etc/samba/smb.conf [----
#===== Gl
[global]
workgroup = WORKGROUP
netbios name = ValeriiAstra
security = user
passdb backend = tdbsam
server min protocol = NT1
client min protocol = NT1
min protocol = NT1

```

Рис 14.

2.3. Создать учетную запись пользователя Samba.

Создадим учетную запись пользователя Samba. Для этого используем команду `smbpasswd` с ключом `-a`.

```

valerii@ValeriiAstra:~$ sudo smbpasswd -a valerii
New SMB password:
Retype new SMB password:
Added user valerii.

```

Рис 15.

Получим информацию об учетной записи командой `pdbedit`.

```

valerii@ValeriiAstra:~$ sudo pdbedit -r valerii
Unix username:      valerii
NT username:
Account Flags:      [U                ]
User SID:           S-1-5-21-2830684959-2925471113-4203666507-1000
Primary Group SID:  S-1-5-21-2830684959-2925471113-4203666507-513
Full Name:
Home Directory:     \\valeriiastra\valerii
HomeDir Drive:
Logon Script:
Profile Path:       \\valeriiastra\valerii\profile
Domain:             VALERIIASTRA
Account desc:
Workstations:
Munged dial:
Logon time:         0
Logoff time:        Ср, 06 фев 2036 18:06:39 MSK
Kickoff time:       Ср, 06 фев 2036 18:06:39 MSK
Password last set:  Пн, 06 мар 2023 12:27:32 MSK
Password can change: Пн, 06 мар 2023 12:27:32 MSK
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

```

Рис 16.

При применении ключа `-r` в команде `pdbedit` возможно просмотреть множество параметров учетной записи в БД `samba`, например, `SID` пользователя, время последней смены пароля и т.д.

2.4. Внутри локального каталога /pub сформировать каталог для выделения в сетевой доступ по smb протоколу

Создадим локальный каталог /pub внутри которого сформируем каталог "SMB_SUKHORUKOV". В последнем создадим текстовый файл "Valerii.txt".

```
valerii@ValeriiAstra:~$ sudo mkdir /pub
valerii@ValeriiAstra:~$ sudo mkdir /pub/SMB_SUKHORUKOV
valerii@ValeriiAstra:~$ cd /pub/SMB_SUKHORUKOV
valerii@ValeriiAstra:/pub/SMB_SUKHORUKOV$ sudo touch Valerii.txt
valerii@ValeriiAstra:/pub/SMB_SUKHORUKOV$ ls
Valerii.txt
```

Рис 17.

Теперь внесем созданный сетевой ресурс " SMB_SUKHORUKOV " со следующими параметрами в файл smb.conf

```
[SMB_SUKHORUKOV]
path=/pub/SMB_SUKHORUKOV
browseable = yes
read only = no
public = yes
valid users = valerii
```

Рис 18.

Проверим корректность конфигурации командой testparm. Параметры секции [global] и секции [SMB_SUKHORUKOV] применились корректно.

```
root@ValeriiAstra:/# testparm
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Registered MSG_REQ_POOL_USAGE
Registered MSG_REQ_DMALLOC_MARK and LOG_CHANGED
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Processing section "[SMB_SUKHORUKOV]"
Loaded services file OK.
Server role: ROLE_STANDALONE
```

Рис 19.

```
[global]
client min protocol = NT1
log file = /var/log/samba/log.%m
logging = file
map to guest = Bad User
max log size = 1000
obey pam restrictions = Yes
pam password change = Yes
panic action = /usr/share/samba/panic-action %d
passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n *
password\updated\ssuccessfully* .
passwd program = /usr/bin/passwd %u
security = USER
server min protocol = NT1
server role = standalone server
unix password sync = Yes
usershare allow guests = Yes
idmap config * : backend = tdb
```

Рис 20.

```
[SMB_SUKHORUKOV]
    guest ok = Yes
    path = /pub/SMB_SUKHORUKOV
    read only = No
    valid users = valerii
```

Рис 21.

2.5. Подготовить условия для подключения smb-клиентов и стартовать сервер Samba.

Отключим межсетевой экран командой **systemctl stop ufw**, и проверим его состояние командой **systemctl status ufw**. Межсетевой экран успешно отключился.

```
root@ValeriiAstra:/# systemctl stop ufw
root@ValeriiAstra:/# systemctl status ufw
• ufw.service - Uncomplicated firewall
   Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Mon 2023-03-06 13:43:29 MSK; 2s ago
     Docs: man:ufw(8)
   Process: 4996 ExecStop=/lib/ufw/ufw-init stop (code=exited, status=0/SUCCESS)
    Main PID: 272 (code=exited, status=0/SUCCESS)

feb 21 10:29:19 ValeriiAstra systemd[1]: Started Uncomplicated firewall.
mar 06 13:43:29 ValeriiAstra systemd[1]: Stopping Uncomplicated firewall...
mar 06 13:43:29 ValeriiAstra ufw-init[4996]: Skip stopping firewall: ufw (not enabled)
mar 06 13:43:29 ValeriiAstra systemd[1]: Stopped Uncomplicated firewall.
```

Рис 22.

Запустим сервер Samba.

```
root@ValeriiAstra:/# systemctl start smbd
root@ValeriiAstra:/# systemctl start nmbd
```

Рис 23.

В списке процессов найдем нужные процесс-демоны, используя команду **ps -x**. Демоны smdb и nmbd успешно запустились.

```
3712 ?      Ss      0:00 /usr/sbin/smbd --foreground --no-process-group
3715 ?      S       0:00 /usr/sbin/smbd --foreground --no-process-group
3716 ?      S       0:00 /usr/sbin/smbd --foreground --no-process-group
3717 ?      S       0:00 /usr/sbin/smbd --foreground --no-process-group
3758 ?      Ss      0:00 /usr/sbin/nmbd --foreground --no-process-group
```

Рис 24.

2.6. В Windows-клиенте проверить доступность и свойства сетевых ресурсов.

2.6.1. Подключение ресурса

Чтобы проверить доступность нашего созданного сетевого ресурса попробуем подключить сетевой диск. Обратимся к Linux узлу по NetBIOS имени.

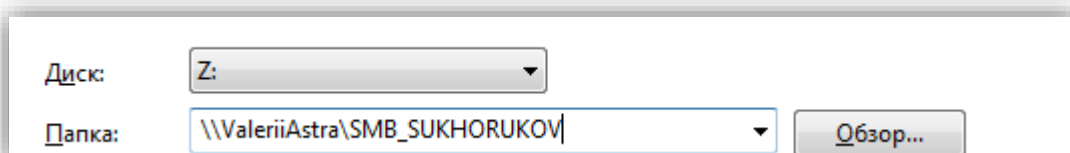


Рис 25.

Далее необходимо указать данные учетной записи. Укажем данные учетной записи Samba.

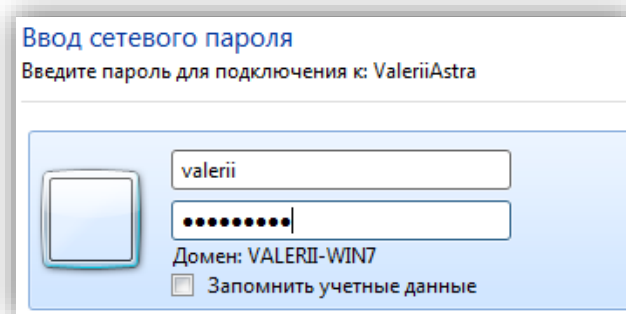


Рис 26.

Результатом успешных настроек двух узлов является доступ к сетевому ресурсу.

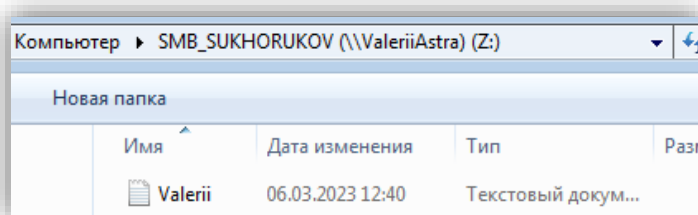


Рис 27.

2.6.2. Проверка прав на подключение

Создадим новую учетную запись Samba, и попробуем получить доступ к сетевому ресурсу на узле Windows.

Создадим локальную учетную запись пользователя командой `adduser`.

```
root@ValeriiAstra:/# adduser sukhorukov2
Добавляется пользователь «sukhorukov2» ...
Добавляется новая группа «sukhorukov2» (1002) ...
```

Рис 28.

Создадим учетную запись Samba с таким же именем.

```
root@ValeriiAstra:/# sudo smbpasswd -a sukhorukov2
New SMB password:
Retype new SMB password:
Added user sukhorukov2.
```

Рис 29.

Попробуем подключиться к ресурсу, явно указав данные новой учетной записи.

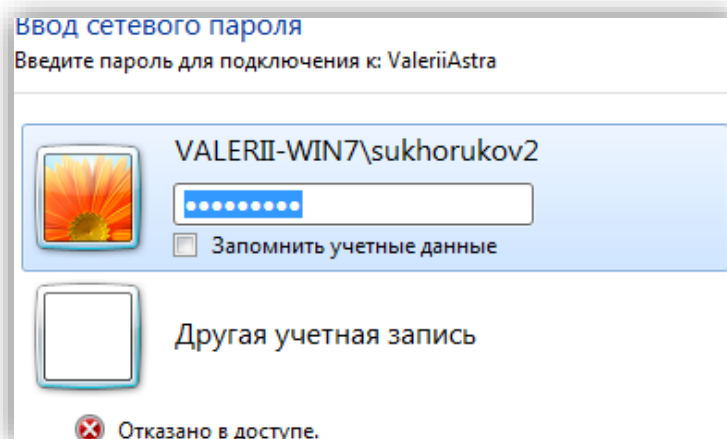


Рис 30.

В доступе было отказано. Это произошло из-за того, что при выделении ресурса в общей доступ в параметре «valid users» была указана одна учетная запись valerii. Добавим в этот список новую учетную запись, и проверим возможность доступа.

```
[SMB_SUKHORUKOV]
path=/pub/SMB_SUKHORUKOV
browseable = yes
read only = no
public = yes
valid users =valerii,sukhorukov2
```

Рис 31.

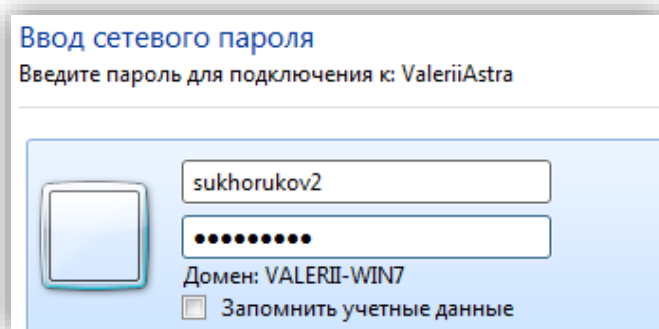


Рис 32.

После добавления учетной записи в список разрешённых, удалось получить доступ с помощью неё.

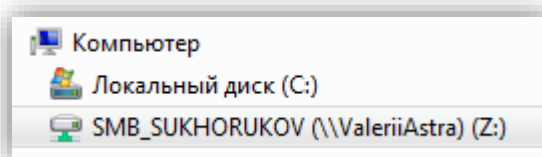


Рис 33.

2.6.3. Разрешения доступа к каталогу

Просмотрим информацию о разрешениях доступа и владельце подключенного ресурса. Владельцем является Unix пользователь root. Разрешения доступа установлены для группы пользователей «Все» по чтению, группы «Unix Group\root» - по чтению, учетной записи «Unix User\root» - полный доступ. Наследование разрешений отключено, все разрешения действуют только для текущего каталога.

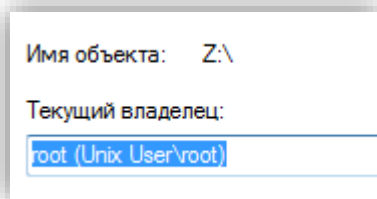


Рис 34.

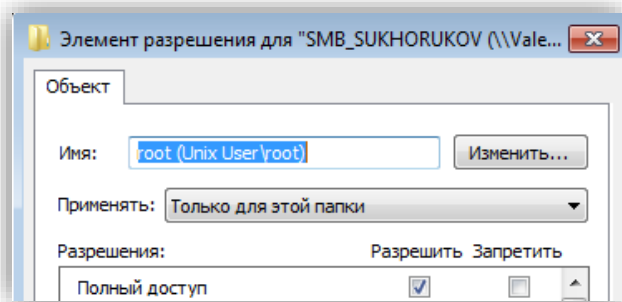


Рис 35.

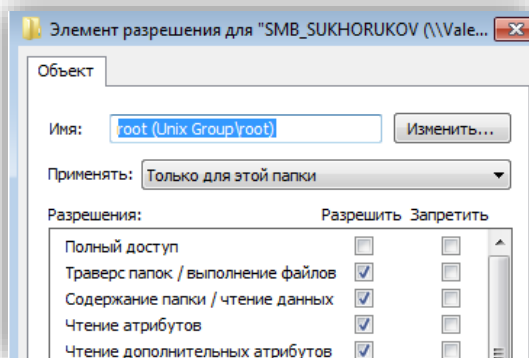


Рис 36.

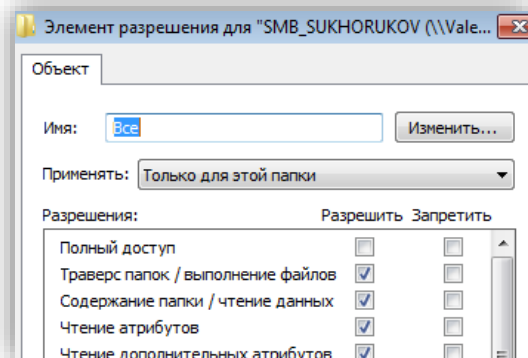


Рис 37.

При выделении каталога в общий доступ параметру «read only» было присвоено значение «по», однако доступ к каталогу доступен только по чтению, при попытке создать файл внутри подключенного каталога возникает ошибка.

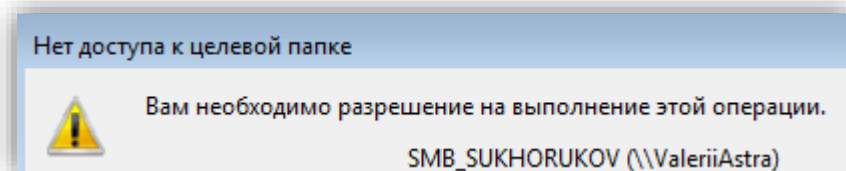


Рис 38.

Посмотрим локальные разрешения каталога на узле Linux.

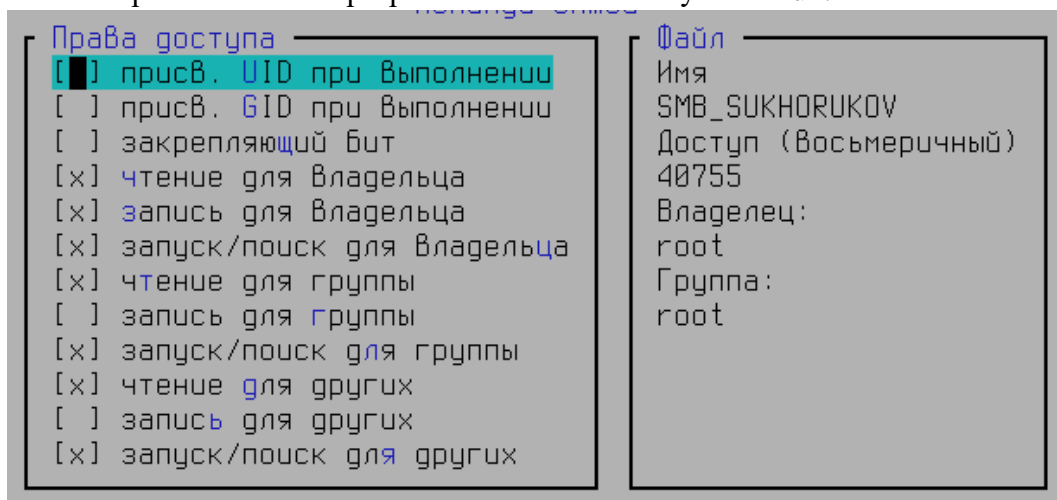


Рис 39.

Для владельца root установлены разрешения полного доступа, для других пользователей установлены разрешения на чтения. Установим разрешение на «запись для других». После этого на узле Windows изменилось отображение прав для группы «Все» (Рис 40).

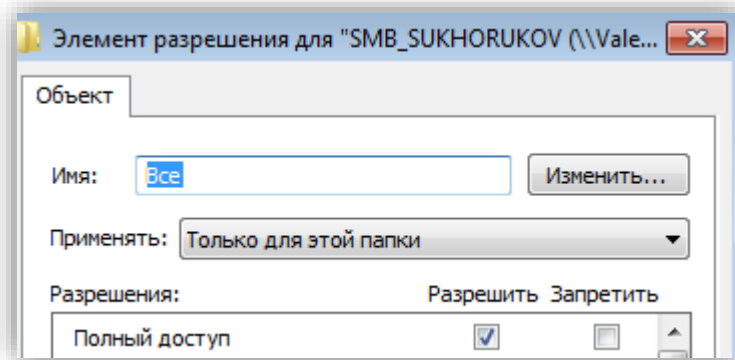


Рис 40.

Создадим новый текстовый документ и посмотрим на узле Linux права доступа.

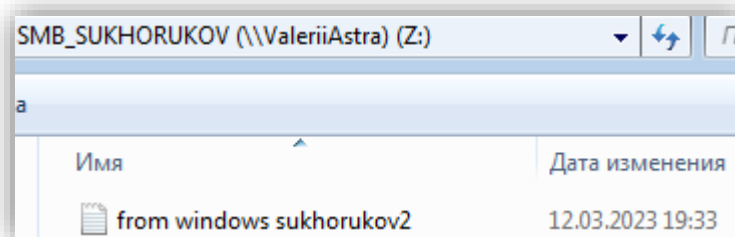


Рис 41.

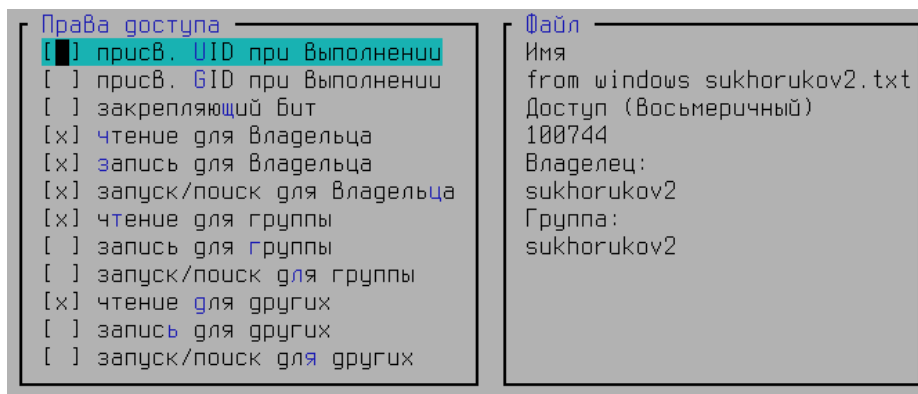


Рис 42.

Владельцем файла является учетная запись sukhorukov2. У данной учетной записи полный доступ к файлу, у других только на чтение.

2.6.4. Проверка отображения содержимого

Запишем в файл информацию на русском и английском языке.

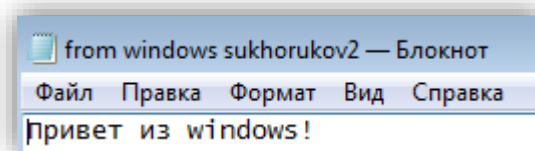


Рис 43.

На Linux узле русский текст отображается некорректно из-за использования разных кодировок на разных ОС.

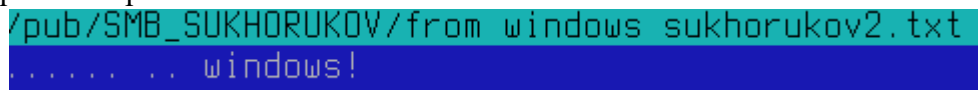


Рис 44.

На Linux изменим файл, добавив новые строки.

```
/pub/SMB_SUKHORUKOV/from windows sukhorukov2.txt
..... .. windows!
"Мой дядя самых честных правил,
Когда не в шутку занемог,
Он уважать себя заставил
И лучше выдумать не мог"
```

Рис 45.

На Windows узле посмотрим содержимое файла. Русский язык также отображается некорректно, и содержимое файла представляется одной строкой. Это связано с разной кодировкой переноса строки на Windows и Linux.

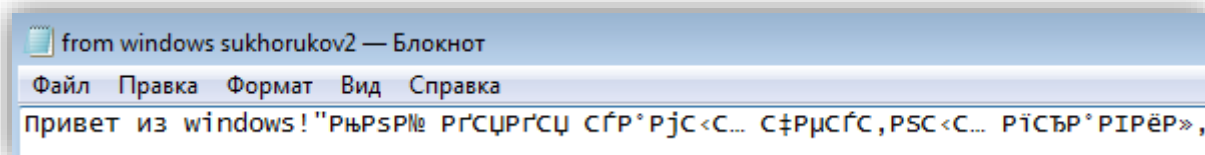


Рис 46.

2.7. Схема сетевого взаимодействия (SMB, Клиент –Windows, Сервер - Linux)

Составим схему сетевого взаимодействия узлов.

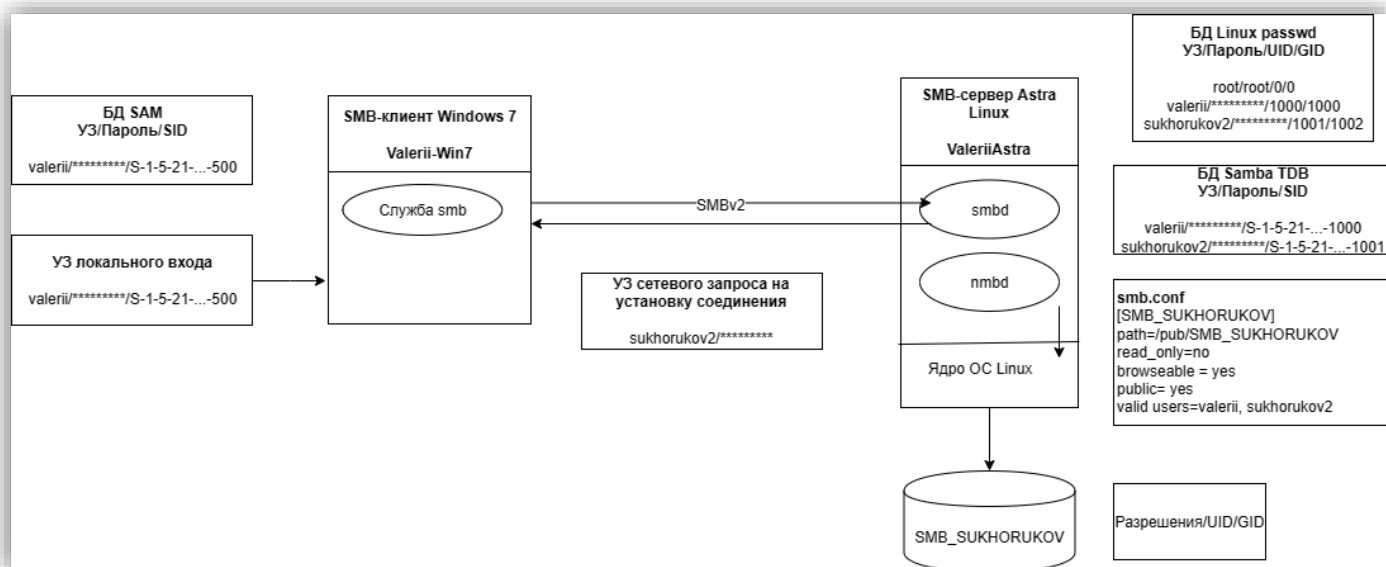


Рис 47.

1. Клиент SMB авторизуется на узле Windows с помощью локальной учетной записи, находящейся в БД SAM.
2. При обращении к серверу SMB клиент авторизуется с помощью УЗ, находящейся в БД Samba на сервере.
3. Служба smb на клиенте обращается к процессу smbd на сервере по протоколу SMBv2.
4. Демон smbd сопоставляет полученные данные УЗ с БД Samba. При совпадении данных и наличии разрешения доступа к ресурсу в файле smb.conf у данной учетной записи происходит отображение УЗ Samba на локальную учетную запись БД passwd.
5. Происходит обращение к ядру Linux для проверки разрешений доступа к запрашиваемому ресурсу. Если разрешения доступа соответствуют запрашиваемой операции, то клиенту предоставляется доступ к ресурсу.

3. Работа SMB-клиента в Linux

3.1. Использование команды smbclient

Отобразим доступные ресурсы для учетной записи sukhorukov2 на сервере Linux с помощью утилиты smbclient.

```
root@ValeriiAstra:/# smbclient -L //ValeriiAstra -U sukhorukov2
Enter WORKGROUP\sukhorukov2's password:

      Sharename      Type            Comment
      -----
      print$         Disk            Printer Drivers
      SMB_SUKHORUKOV Disk            Home Directories
      IPC$           IPC            IPC Service (Samba 4.9.5-Debian)
      sukhorukov2    Disk            Home Directories
```

Рис 48.

- ❖ Print\$ - используется для общего доступа к принтерам в рабочей группе.
- ❖ SMB_SUKHORUKOV – созданный ресурс.
- ❖ IPC\$ - используется при организации временных подключений, создаваемых приложениями для обмена данными с помощью именованных каналов.
- ❖ sukhorukov2 – домашний каталог пользователя на узле Linux.

Подключимся с помощью данной утилиты к ресурсу SMB_SUKHORUKOV.

```
root@ValeriiAstra:/# smbclient //ValeriiAstra/SMB_SUKHORUKOV -U sukhorukov2
Enter WORKGROUP\sukhorukov2's password:
Try "help" to get a list of possible commands.
smb: \>
```

Рис 49.

После подключения можно выполнять разовые отладочные действия с каталогом. Опробуем на практике основные команды:

- ❖ ls- позволяет посмотреть структуру каталога со всеми файлами и подкаталогами.

```
smb: \> ls
.                D          0  Sun Mar 12 19:46:22 2023
..               D          0  Mon Mar  6 12:40:06 2023
Valerii.txt      N          0  Mon Mar  6 12:40:54 2023
from windows sukhorukov2.txt  A        213  Sun Mar 12 19:46:22 2023
23606672 blocks of size 1024. 15934672 blocks available
```

Рис 50.

- ❖ get- копирует файл с сервера. Скопируем текстовый файл "from windows sukhorukov2", который был создан на Windows машине, в домашний каталог пользователя.

```
smb: \> get "from windows sukhorukov2.txt" /home/sukhorukov2/test.txt
getting file \from windows sukhorukov2.txt of size 213 as /home/sukhorukov2/test.txt (213000
0,0 KiloBytes/sec) (average inf KiloBytes/sec)
```

Рис 51.

<- /home/sukhorukov2 .[^]>			
.u	Имя	Размер	Время правки
/..		-BBEPX-	мар 12 14:02
/Desktop		4096	мар 12 14:02
.bash_logout		220	мар 12 14:02
.bashrc		3526	мар 12 14:02
.profile		675	мар 12 14:02
test.txt		213	мар 13 10:59

Рис 52.

- ❖ del- удаление файла с сервера. Удалим текстовый файл "valerii.txt".

```
smb: \> del Valerii.txt
smb: \> ls
.                D          0 Mon Mar 13 11:03:18 2023
..               D          0 Mon Mar  6 12:40:06 2023
from windows sukhorukov2.txt  A        213 Sun Mar 12 19:46:22 2023
```

Рис 53.

- ❖ history- выводит историю выполнения команд.

```
smb: \> history
0: help
1: ls
2: get "from windows sukhorukov2.txt" /home/sukhorukov2/test.txt
3: del Valerii.txt
4: ls
5: history
```

Рис 54.

- ❖ allinfo- выводит всю информацию о файле или каталоге.

```
smb: \> allinfo "from windows sukhorukov2.txt"
altname: FWH6NP~3.TXT
create_time:      Bc мар 12 19:33:01 2023 MSK
access_time:      Bc мар 12 19:46:31 2023 MSK
write_time:       Bc мар 12 19:46:22 2023 MSK
change_time:      Bc мар 12 19:46:22 2023 MSK
attributes: A (20)
stream: [::$DATA], 213 bytes
```

Рис 55.

3.2. Использование команды smbtree

smbtree — это программа-браузер smb в текстовом режиме. Она похожа на «Сетевое окружение» на ОС Windows. Программа отображает дерево со всеми известными доменами и рабочими группами, компьютерами в этих доменах и группах, и общими ресурсами на компьютерах.

С помощью команды `smbtree` выполним обзор smb-ресурсов.

```
root@ValeriiAstra:/# smbtree
WORKGROUP
  \\VALERIIASTRA
    Samba 4.9.5-Debian
    \\VALERIIASTRA\IPC$ IPC Service (Samba 4.9.5-Debian)
    \\VALERIIASTRA\SMB_SUKHORUKOV
    \\VALERIIASTRA\print$ Printer Drivers
  \\VALERII-WIN7
  \\VALERII-PC
```

Рис 56.

В сети была найдена рабочая группа `WORKGROUP`, и три компьютера – две виртуальных, и одна основная машина. Условием работы данной программы является включенный протокол `SMBv1`. Данный протокол был разрешен при конфигурировании Samba в секции `[global]`.

3.3. Использование команды `mount.cifs`

Для использования команды `mount.cifs` установим компонент `cifs-utils`.

```
root@ValeriiAstra:/# apt-get install cifs-utils
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Предлагаемые пакеты:
  winbind
НОВЫЕ пакеты, которые будут установлены:
  cifs-utils
```

Рис 57.

Выполним монтирование каталога `SMB_SUKHORUKOV` в каталог `/mnt/smb`

```
root@ValeriiAstra:/# mount.cifs //ValeriiAstra/SMB_SUKHORUKOV /mnt/smb -o user=sukhorukov2
Password for sukhорukov2@//ValeriiAstra/SMB_SUKHORUKOV: *****
```

Рис 58.

Подключенный ресурс успешно подключился.

```
root@ValeriiAstra:/# ls /mnt/smb
from windows sukhорukov2.txt
```

Рис 59.

3.4. Использование команды smbstatus

Для отображения состояния smb-сеанса на сервере используем команду smbstatus.

```
root@ValeriiAstra:/# smbstatus

Samba version 4.9.5-Debian
PID      Username   Group      Machine                                     Protocol Version Encryption      Signing
-----
1583     sukhorukov2 sukhorukov2 127.0.0.1 (ipv4:127.0.0.1:45630)          SMB3_11      -              partial(AES-128-CMAC)

Service  pid      Machine    Connected at                               Encryption  Signing
-----
SMB_SUKHORUKOV 1583     127.0.0.1  Пн мар 13 12:18:40 2023 MSK -      -
IPC$      1583     127.0.0.1  Пн мар 13 12:18:40 2023 MSK -      -

No locked files
```

Рис 60.

Результатом выполнения является список учетных записей пользователей, IP адресов машин, с которой произошло подключение, и список используемых сетевых ресурсов.

Рассмотрим протоколы демонов samba, которые хранятся в каталоге /var/log/samba.

```
<- /var/log/samba .[~]>
.u          Имя
/..         -ВВЕРХ-
/cores      4096
log.        0
log.127.0.0.1 0
log.192.168.0.103 0
log.192.168.0.108 0
log.nmbd    722
log.smbd    336
log.valerii-win7 0
log.valeriiastra 0
log.valeriiastra 0
```

Рис 61.

log.smbd и log.nmbd содержат информация о включении/выключении nmbd и smbd демонов. Также в файле log.nmbd содержатся сообщения, связанные с функционалом Samba NETBIOS over IP, в log.smbd - сообщения, связанные с функционалом Samba SMB/CIFS.

```
/var/log/samba/log.nmbd
[2023/03/06 11:12:37.101285, 0] ../lib/util/become_daemon.c:138(daemon_ready)
daemon_ready: STATUS=daemon 'nmbd' finished starting up and ready to serve connections
[2023/03/12 23:22:06.806435, 0] ../source3/nmbd/nmbd_namequery.c:109(query_name_response)
query_name_response: Multiple (2) responses received for a query on subnet 192.168.0.108 for name WORKGROUP<id>
This response was from IP 192.168.0.1, reporting an IP address of 192.168.0.1.
[2023/03/13 11:59:15.232274, 0] ../source3/nmbd/nmbd.c:58(terminate)
Got SIGTERM: going down...
[2023/03/13 12:04:01.568206, 0] ../lib/util/become_daemon.c:138(daemon_ready)
daemon_ready: STATUS=daemon 'nmbd' finished starting up and ready to serve connections
```

Рис 62.

```
/var/log/samba/log.smbd
[2023/03/06 11:12:36.892435, 0] ../lib/util/become_daemon.c:138(daemon_ready)
daemon_ready: STATUS=daemon 'smbd' finished starting up and ready to serve connections
[2023/03/13 12:04:06.129289, 0] ../lib/util/become_daemon.c:138(daemon_ready)
daemon_ready: STATUS=daemon 'smbd' finished starting up and ready to serve connections
```

Рис 63.

3.5. Схема сетевого взаимодействия (SMB, Клиент –Linux, Сервер - Linux)

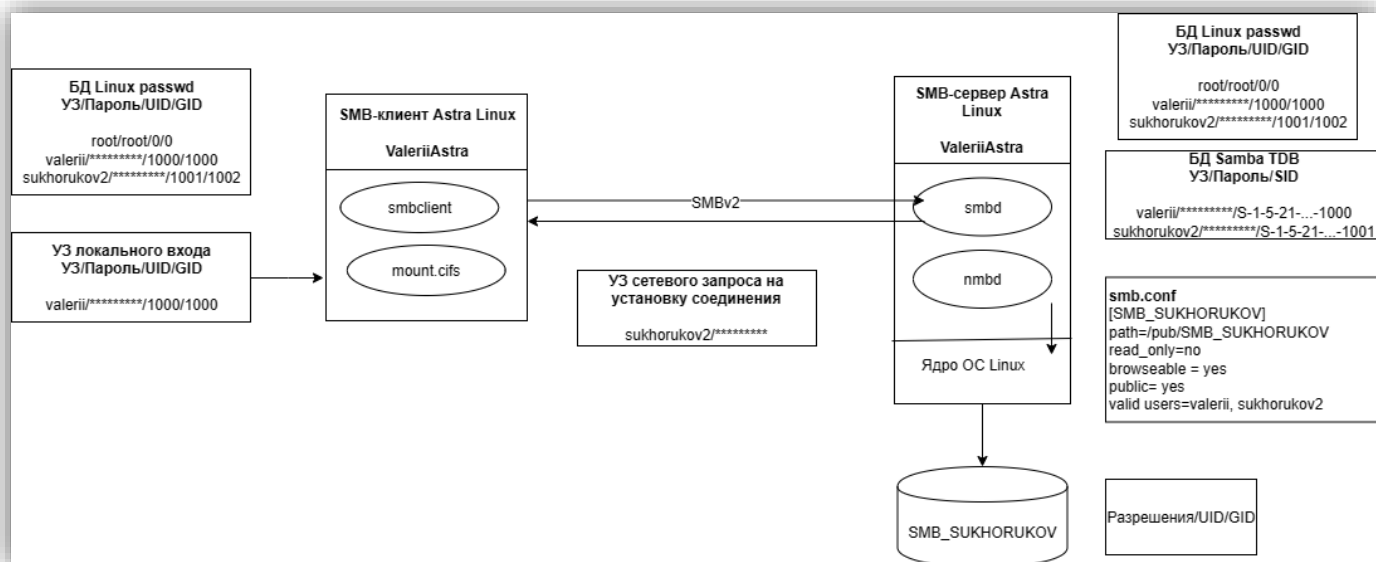


Рис 64.

1. Клиент SMB авторизуется на узле Linux с помощью локальной учетной записи, находящейся в БД passwd.
2. При обращении к серверу SMB клиент авторизуется с помощью УЗ, находящейся в БД Samba на сервере.
3. Служба mount.cifs или smbclient на клиенте обращается к процессу smb на сервере по протоколу SMBv2.
4. Демон smb сопоставляет полученные данные УЗ с БД Samba. При совпадении данных и наличии разрешения доступа к ресурсу в файле smb.conf у данной учетной записи происходит отображение УЗ Samba на локальную учетную запись БД passwd.
5. Происходит обращение к ядру Linux для проверки разрешений доступа к запрашиваемому ресурсу. Если разрешения доступа соответствуют запрашиваемой операции, то клиенту предоставляется доступ к ресурсу.

4. Использование команды net.

Утилита net используется для администрирования локальными и удаленными серверами Samba. Данная утилита по принципу работы похожа на команду net, входящую в состав Windows.

Рассмотрим и опробуем информационные возможности утилиты:

- ❖ net getlocalsid- позволяет получить SID данного сервера.

```
root@ValeriiAstra:/# net getlocalsid
SID for domain VALERIIASTRA is: S-1-5-21-2830684959-2925471113-4203666507
```

Рис 65.

- ❖ net lookup имя_хоста- позволяет узнать по имени хоста его IP-адрес.

```
root@ValeriiAstra:/# net lookup Valerii-Win7
192.168.0.103
```

Рис 66.

- ❖ net status sessions- выводит информацию о сессиях.

```
root@ValeriiAstra:/# net status sessions
PID      Username      Group        Machine
-----
1583     sukhorukov2   sukhorukov2  127.0.0.1    (ipv4:127.0.0.1:45630)
```

Рис 67.

2 Часть. Взаимодействие на базе протокола NFS

5. Сетевая файловая система NFS в Linux.

5.1. Найти основные компоненты, необходимые для работы NFS

Network File System (NFS) — протокол сетевого доступа к файловым системам, первоначально разработан Sun Microsystems в 1984 году. За основу взят протокол вызова удалённых процедур (ONC RPC, англ. Open Network Computing Remote Procedure Call). Позволяет монтировать (подключать) удалённые файловые системы через сеть.

Для установки сервера nfs на узле Linux выполним команду **sudo apt-get install nfs-kernel-server**

```
root@ValeriiAstra:/# apt-get install nfs-kernel-server
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  libevent-2.0-5 libnfsidmap2 nfs-common rpcbind
```

Рис 68.

Для установки клиента nfs на узле Linux выполним команду **sudo apt-get install nfs-kernel-server**

```
root@ValeriiAstra:/# apt-get install nfs-common
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Уже установлен пакет nfs-common самой новой версии (1:1.3.4-2.1+deb9u1).
```

Рис 69.

Клиентская часть установилась вместе с серверной.

Рассмотрим основные компоненты nfs.

/etc/...

- ❖ exports - Конфигурационный файл nfs, содержит список экспортируемых файловых систем.

- ❖ nfsmount.conf - Конфигурационный файл, позволяет установить опции монтирования глобально, для каждого сервера или для каждой точки монтирования.

- ❖ mtab - содержат информацию о смонтированных файловых системах

/usr/sbin/...

- ❖ rpc.nfsd - Основной процесс NFS сервера.

- ❖ rpc.mountd - NFS демон монтирования.

- ❖ rpc.statd - Демон мониторинга статуса хостов.
- ❖ rpcbind (portmapper) - Утилита, конвертирующая RPC номер программы в универсальный адрес.
- ❖ rpcinfo – Утилита получения информации о RPC
- ❖ exportfs - Утилита, обслуживающая таблицу экспортированных NFS файловых систем.

5.2. Выделение каталога в общий доступ

Создадим каталог "nfs" внутри локального каталога /pub для сетевого доступа по NFS, в нём создадим текстовый файл "Sukhorukov".

```
root@ValeriiAstra:/# mkdir /pub/nfs
root@ValeriiAstra:/# cd /pub/nfs
root@ValeriiAstra:/pub/nfs# touch Sukhorukov.txt
root@ValeriiAstra:/pub/nfs# ls
Sukhorukov.txt
```

Рис 70.

Опишем экспорт каталога в /etc/exports.

```
/etc/exports [-M--] 0 L:[ 1+
# /etc/exports: the access control l
#<----->X<----->to NFS clients. See
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync
# /srv/nfs4/homes gss/krb5i(rw,sync
#
# /pub/nfs *(rw,sync,no_root_squash)
```

Рис 71.

К каталогу можно подключиться с помощью любой учетной записи. Доступ предоставлен по чтению и по записи. Опция no_root_squash используется для доступа root по сети.

Обновим таблицу экспорта в ядре командой **exportfs -r**. В файле /var/lib/nfs/etab содержится полная информация и ресурсах, к которым предоставлен доступ по nfs.

```
/var/lib/nfs/etab [----] 0 L:[ 1+ 1 2/ 2] *(196 / 196b) <EOF>
/pub/nfs<----->*(rw,sync,wdelay,hide,nocrossmnt,secure,no_root_squash,no_all_squash,no_subtree_check,
```

Рис 72.

5.3. Запуск NFS

Перезапустим демоны NFS командой **systemctl restart nfs-server**. Проверим статус командой **systemctl status nfs-server**.

```
root@ValeriiAstra:/# systemctl status nfs-server
• nfs-server.service - NFS server and services
   Loaded: loaded (/lib/systemd/system/nfs-server.service; enabled; vendor preset: enabled)
   Active: active (exited) since Mon 2023-03-13 17:50:53 MSK; 10min ago
```

Просмотрим запущенные процессы командой **ps -ax**, и найдем нужные демоны.

```
1539 ?      Ss      0:00 /usr/sbin/rpc.idmapd
1540 ?      Ss      0:00 /usr/sbin/rpc.mountd --manage-gids
1548 ?      S       0:00 [lockd]
1551 ?      S       0:00 [nfsd]
1552 ?      S       0:00 [nfsd]
1553 ?      S       0:00 [nfsd]
1554 ?      S       0:00 [nfsd]
1555 ?      S       0:00 [nfsd]
1556 ?      S       0:00 [nfsd]
1557 ?      S       0:00 [nfsd]
1558 ?      S       0:00 [nfsd]
```

Рис 73.

Определим протоколы и порты сервисов NFS командой **rpcinfo -p**.

```
root@ValeriiAstra:/# rpcinfo -p
  program vers proto  port  service
    100000   4    tcp   111   portmapper
    100000   3    tcp   111   portmapper
    100000   2    tcp   111   portmapper
    100000   4    udp   111   portmapper
    100000   3    udp   111   portmapper
    100000   2    udp   111   portmapper
    100005   1    udp  47601 mountd
    100005   1    tcp  36037 mountd
    100005   2    udp  47597 mountd
    100005   2    tcp  41213 mountd
    100005   3    udp  45091 mountd
    100005   3    tcp  51901 mountd
    100003   3    tcp   2049  nfs
    100003   4    tcp   2049  nfs
    100227   3    tcp   2049
    100003   3    udp   2049  nfs
    100227   3    udp   2049
    100021   1    udp  56736 nlockmgr
    100021   3    udp  56736 nlockmgr
    100021   4    udp  56736 nlockmgr
    100021   1    tcp  43425 nlockmgr
    100021   3    tcp  43425 nlockmgr
    100021   4    tcp  43425 nlockmgr
```

Рис 74.

Сервисы NFS работают как по протоколу TCP, так и по протоколу UDP разных версий.

5.4. Монтирование сетевой файловой системы

Произведем монтирование в каталог /mnt/nfs. Для этого используем команду mount.

```
root@ValeriiAstra:/# mount -t nfs -o soft ValeriiAstra:/pub/nfs /mnt/nfs
root@ValeriiAstra:/# cd /mnt/nfs
root@ValeriiAstra:/mnt/nfs# ls
Sukhorukov.txt
```

Рис 75.

Монтирование произошло успешно. С помощью команды mount без параметров найдём в списке смонтированную сетевую файловую систему.

```
ValeriiAstra:/pub/nfs on /mnt/nfs type nfs4
```

Рис 76.

Можно увидеть, что при монтировании был использован протокол NFS4. Размонтируем подключенный ресурс командой **umount**.

```
root@ValeriiAstra:/# umount /mnt/nfs
root@ValeriiAstra:/#
```

Рис 77.

5.5. Схема сетевого взаимодействия (NFS, Клиент –Linux, Сервер - Linux)

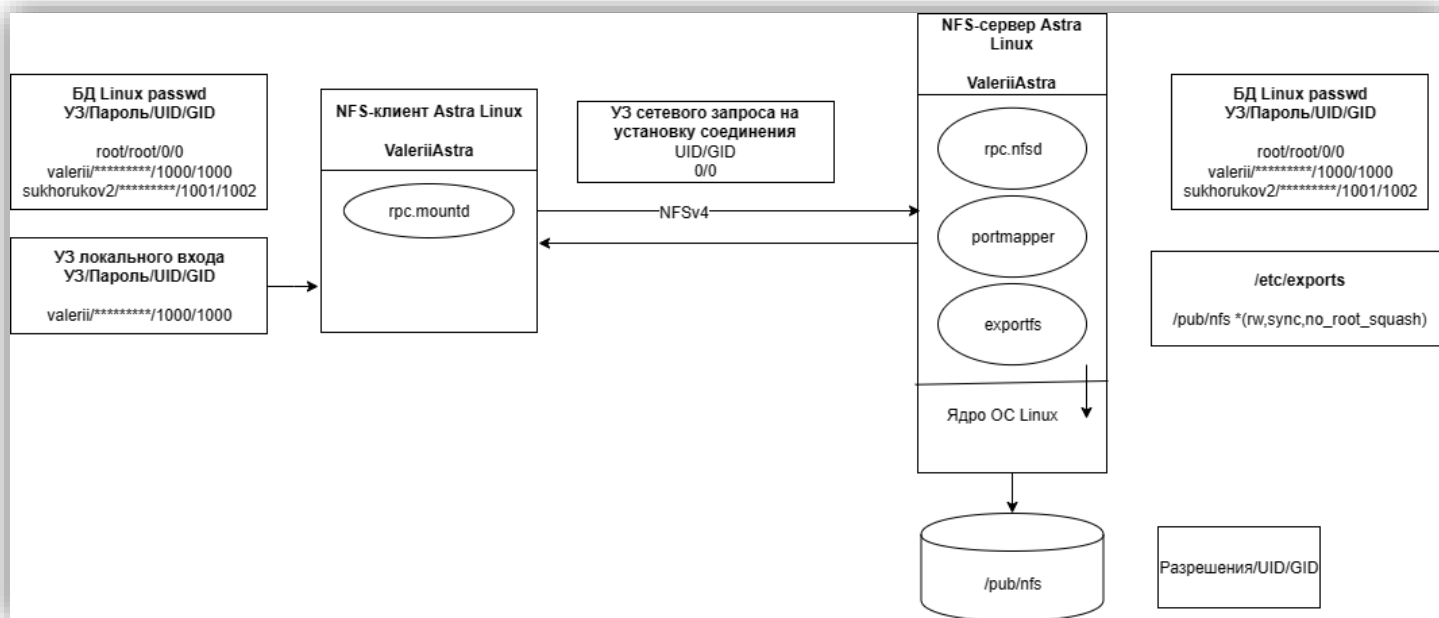


Рис 78.

1. Клиент NFS авторизуется на узле Linux с помощью локальной учетной записи, находящейся в БД passwd.
2. Служба `rpc.mountd` на клиенте обращается к процессу `rpc.nfsd` на сервере по протоколу NFSv4.
3. При обращении к серверу NFS клиент авторизуется с помощью УЗ, находящейся в БД passwd на сервере.

4. Полученные данные УЗ сопоставляются с БД passwd на сервере. При совпадении данных клиент успешно аутентифицируется на сервере.

5. Программа exportfs сопоставляет полученные данные с разрешениями, описанными в файле /etc/exports.

6. При наличии разрешения доступа к сетевому ресурсу, происходит обращение к ядру Linux для проверки разрешений доступа к локальному ресурсу. Если разрешения доступа соответствуют запрашиваемой операции, то клиенту предоставляется доступ к ресурсу.

6. Использование в Windows Server служб Service for NFS для организации сетевого доступа по протоколу NFS.

6.1. Настроить файл-сервер в Windows Server

Роль файл-сервера была установлена на машине VALERII-S-1 при присвоении ей статуса контроллера домена. Установим компонент «Диспетчер ресурсов файлового сервера» и «Службы для NFS».

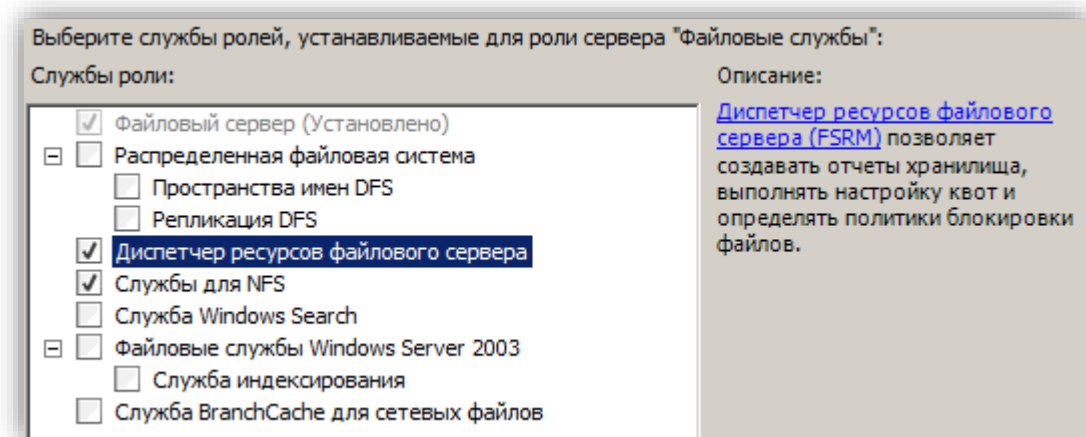


Рис 79.

После установки в меню "Администрирование" появились оснастки "Диспетчер ресурсов файлового сервера" и "Службы для NFS".

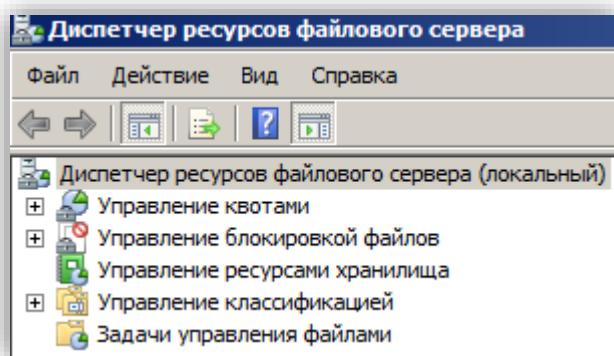


Рис 80.

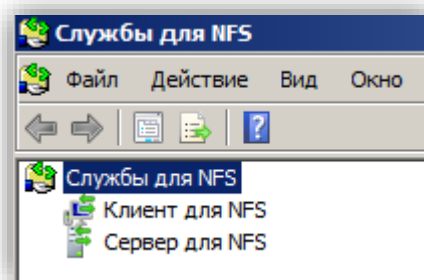


Рис 81.

6.2. Рассмотреть средства согласования учетных записей и свойства службы отображения имен.

Для работы NFS между клиентами и серверами с разными ОС используют механизм согласования учетных записей. Для реализации совместного доступа к ресурсам между Windows и Linux необходимо сопоставить SID учетной записи Windows UID, GID учетной записи Linux.

Создадим в БД AD на контроллере домена в Windows учетную запись с именем sukhorukov2, как на узле Windows.

Новый объект - Пользователь

Создать в: Sukhorukov.com/Users

Имя: sukhorukov2 Инициалы:

Фамилия:

Полное имя: sukhorukov2

Имя входа пользователя: sukhorukov2 @Sukhorukov.com

Имя входа пользователя (пред-Windows 2000): SUKHORUKOV\ sukhorukov2

Рис 82.

Получим UID, GID УЗ в Linux с помощью команды **id**.

```
root@ValeriiAstra:/# id sukhorukov2
uid=1001(sukhorukov2) gid=1002(sukhorukov2)
```

Рис 83.

С помощью оснастки «Редактирование ADSI» настроим согласование учетных записей.

CN=sukhorukov2 - свойства

Редактор атрибутов | Безопасность

Атрибуты:

Атрибут	Значение
gidNumber	1002

Рис 84.

CN=sukhorukov2 - свойства

Редактор атрибутов | Безопасность

Атрибуты:

Атрибут	Значение
uidNumber	1001

Рис 85.

Также установим согласование УЗ «Администратор» с УЗ root, указав uidNumber и gidNumber равные 0.

CN=Администратор - свойства

Редактор атрибутов | Безопасность

Атрибуты:

Атрибут	Значение
gidNumber	0

Рис 86.

CN=Администратор - свойства

Редактор атрибутов | Безопасность

Атрибуты:

Атрибут	Значение
uidNumber	0

Рис 87.

В свойствах «Службы для NFS» для работы сопоставления учетных записей необходимо установить источник. Укажем имя домена Active Directory.

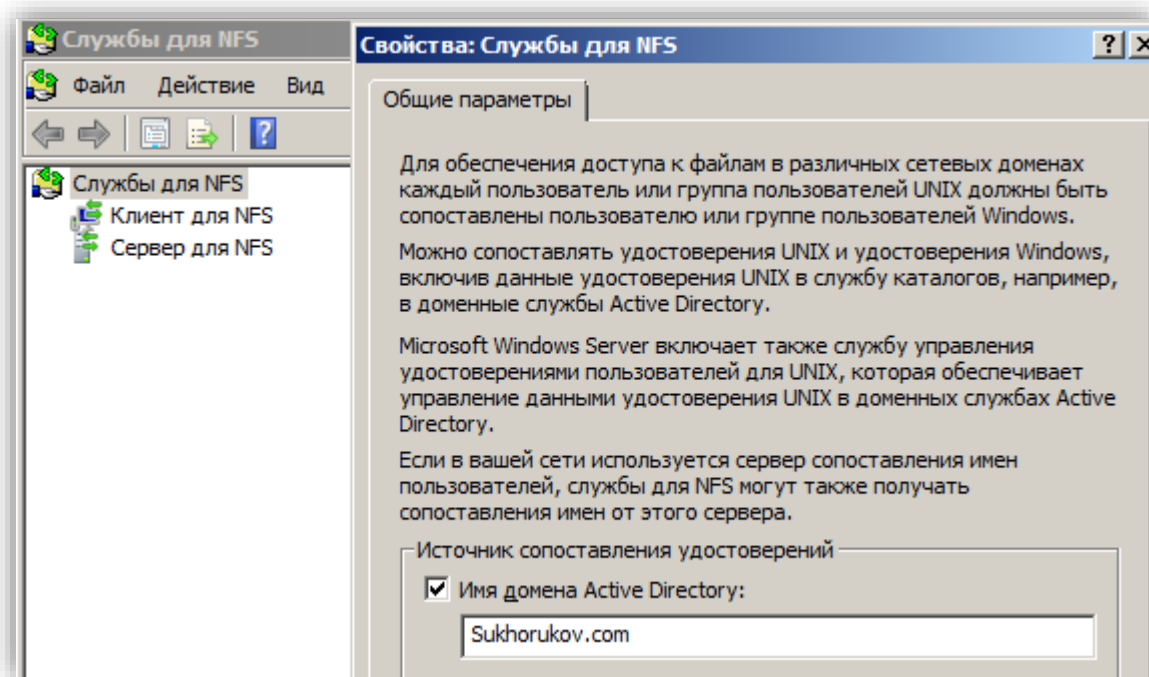


Рис 88.

6.3. Служба «Сервер для NFS»

Разберем свойства службы "Сервер для NFS":

- ❖ **Параметры сервера**- на этой вкладке можно включить/отключить поддержку NFS 3 версии, выбрать транспортный протокол: только UDP, только TCP или TCP+UDP. Также можно задать периодическую проверку данных подлинности пользователей или же вообще ее не выполнять.

- ❖ **Обработка имен файлов**- на этой вкладке можно указать файлы, имена которых нужно преобразовывать для знаков, допустимых в NFS, но недопустимых в NTFS. А также задать дополнительные параметры: создавать файлы, имена которых начинаются с точки, как скрытые и включить/отключить поддержку учета регистра в именах файлов на сервере для NFS.

- ❖ **Блокировка**- на этой вкладке можно указать период ожидания повторного запроса на блокировку после возобновления работы сервера для "Сервер для NFS".

- ❖ **Журнал активности**- на этой вкладке можно выбрать действия, которые будут регистрироваться сервером для NFS: запросы на подключение и отключение, запросы на блокировку и разблокировку, запросы на чтение и запись, запросы на создание и удаление.

- ❖ **Группы сети** - на этой вкладке можно задать поддержку сетевых групп, которые будут использоваться для доступа к общим ресурсам NFS: Сервер NIS или домен AD.

Запустим службу.

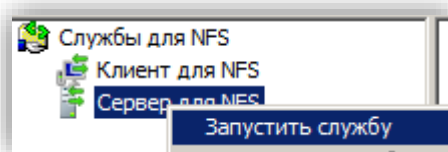


Рис 89.

6.4. На Windows-сервере создать каталог, определить разрешения доступа NTFS. Средствами эксплорера в свойствах каталога настроить параметры экспорта каталога по NFS.

Создадим каталог C:\Users\Администратор\NFS_SUKHRORUKOV и настроим разрешения доступа NTFS – полный доступ для sukhorukov2 и Администратор, чтение и выполнение для остальных пользователей.

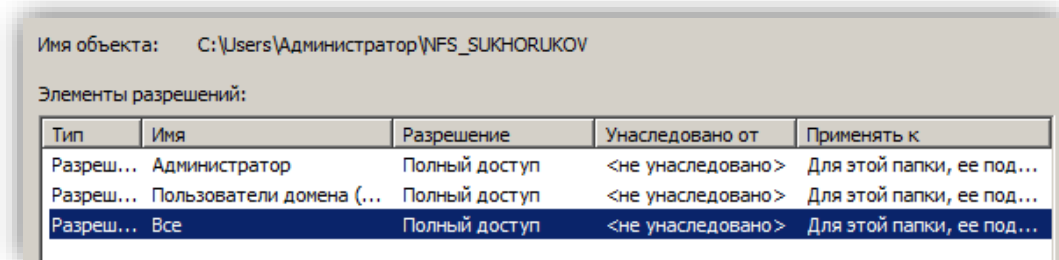


Рис 90.

На вкладке «Совместный доступ NFS» настроим разрешения NFS. Разрешим несопоставленный доступ в варианте «Разрешить несопоставленный доступ пользователям Linux».

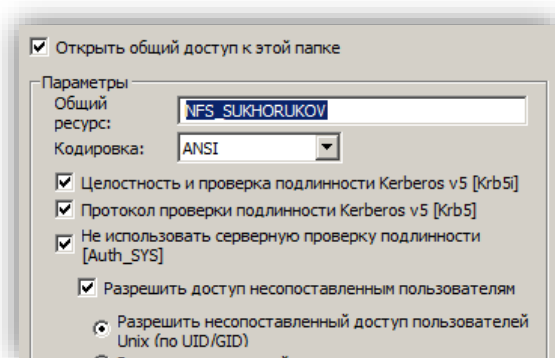


Рис 91.

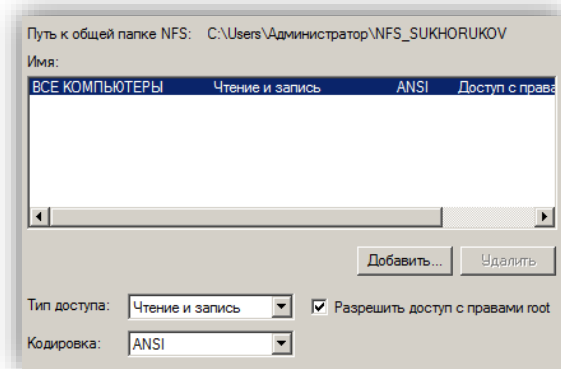


Рис 92.

6.5. На Windows-сервере с помощью консоли администрирования перезапустить сервер NFS. Командой showmount отобразить состояние ресурсов NFS.

Перезапустим сервер NFS и с помощью команды **showmount** отобразим состояние ресурсов NFS.

Ключ **e** отображает все файловые системы, экспортированные на сервере.

Ключ **a** отображает все клиенты NFS и каталоги на сервере, которые подключены.

```
C:\Users\Администратор>showmount -e
Списка экспорта на VALERII-S-1:
/NFS_SUKHRORUKOV           Все компьютеры

C:\Users\Администратор>showmount -a
Все точки подключения на VALERII-S-1:
```

Рис 93.

Так как мы еще не смонтировали наш файловый ресурс, поэтому мы не видим клиентов NFS, которые отображаются командой showmount -a.

6.6. Схема сетевого взаимодействия (NFS, Клиент –Linux, Сервер – Windows, сопоставленный доступ)

Смонтируем на Linux-клиенте файловый ресурс NFS-сервера Windows командой **mount**.

```
root@ValeriiAstra:/# mount -t nfs 192.168.0.111:/NFS_SUKHORUKOV /mnt/nfs
```

Рис 94.

Командой **mount** без параметров получим список смонтированных файловых систем, и найдём смонтированный каталог.

```
192.168.0.111:/NFS_SUKHORUKOV on /mnt/nfs type nfs (rw,relatime,vers=3,rsize=32768,wsizе=32768,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,mountaddr=192.168.0.111,mountvers=3,mountport=1048,mountproto=udp,local_lock=none,addr=192.168.0.111,user=sukhorukov2)
```

Рис 95.

Проверим командой **showmount -a** точки подключения на узле Windows.

```
C:\Users\Администратор>showmount -a
Все точки подключения на VALERII-S-1:
192.168.0.108 : C:\Users\Администратор\NFS_SUKHORUKOV
```

Рис 96.

Каталог успешно смонтировался. Просмотрим права доступа у подключённого каталога.

Права доступа	Файл
[] присв. UID при выполнении	Имя
[] присв. GID при выполнении	nfs
[] закрепляющий бит	Доступ (восьмеричный)
[x] чтение для владельца	40777
[x] запись для владельца	Владелец:
[x] запуск/поиск для владельца	root
[x] чтение для группы	Группа:
[x] запись для группы	root
[x] запуск/поиск для группы	
[x] чтение для других	
[x] запись для других	
[x] запуск/поиск для других	

Рис 97.

Учетная запись «Администратор» сопоставилась с УЗ «root».

Создадим на узле Linux два файла, используя разные учетные записи – root, и sukhorukov2.

```
Имя
ws_asministrator.txt
Доступ (Восьмеричный)
100777
Владелец:
root
Группа:
root
```

Рис 98.

```
Имя
ws_sukhorukov2.txt
Доступ (Восьмеричный)
100777
Владелец:
sukhorukov2
Группа:
sukhorukov2
```

Рис 99.

На Window посмотрим владельца файлов. Сопоставление в файлах работает корректно.

```
Имя объекта: C:\Users\Администратор\NFS_SUKHORUKOV\ws_asministrator.txt
Текущий владелец:
Администратор
```

Рис 100.

```
Имя объекта: C:\Users\Администратор\NFS_SUKHORUKOV\ws_sukhorukov2.txt
Текущий владелец:
sukhorukov2 (sukhorukov2@Sukhorukov.com)
```

Рис 101.

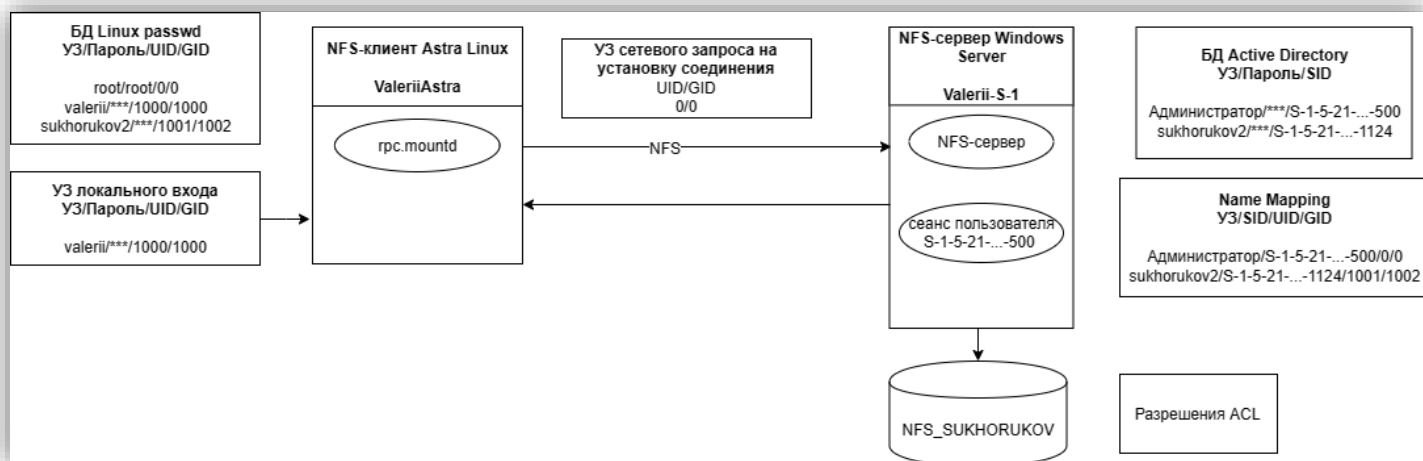


Рис 102.

1. Клиент NFS авторизуется на узле Linux с помощью локальной учетной записи, находящейся в БД passwd.
2. Служба rpc.mountd на клиенте обращается к NFS серверу на узле Windows по протоколу NFS.
3. При обращении к серверу NFS клиент передает UID/GID учетной записи, указанной как параметр подключения (0/0).
4. Полученные UID/GID используются для поиска УЗ в БД AD.
5. Создается сеанс пользователя с sid сопоставленным по uid/gid.

6. При наличии разрешения доступа к локальному ресурсу клиенту предоставляется доступ к ресурсу.

6.7. Схема сетевого взаимодействия (NFS, Клиент –Linux, Сервер – Windows, несопоставленный доступ)

Реализуем несопоставленный доступ. Для этого смонтируем диск от имени учетной записи valerii, для которой нет сопоставления с sid в БД AD на узле Windows Server.

```
valerii@ValeriiAstra:~$ sudo mount -t nfs 192.168.0.111:/NFS_SUKHORUKOV /mnt/nfs -o user=valerii
```

Рис 103.

Создадим в подключенном каталоге файл и посмотрим его разрешения на Windows-сервере.

Запретить	S-1-5-88-3-420	Полный доступ	<не унаследовано>
Разрешить	S-1-5-88-1-1003	Особые	<не унаследовано>
Разрешить	S-1-5-88-2-1004	Чтение	<не унаследовано>
Разрешить	S-1-5-88-4	Чтение	<не унаследовано>
Разрешить	система	Полный доступ	<не унаследовано>

Рис 104.

Учетная запись отобразилась на следующие SIDы:

- ❖ S-1-5-88-1-1003 с разрешениями на полный доступ – SID УЗ пользователя-владельца.
- ❖ S-1-5-88-2-1004 с разрешениями на чтение – SID группы-владельца.
- ❖ S-1-5-88-4 с разрешениями на чтение – SID для УЗ остальных пользователей.
- ❖ S-1-5-88-3-420 с запретом на полный доступ – SID для особых разрешений.

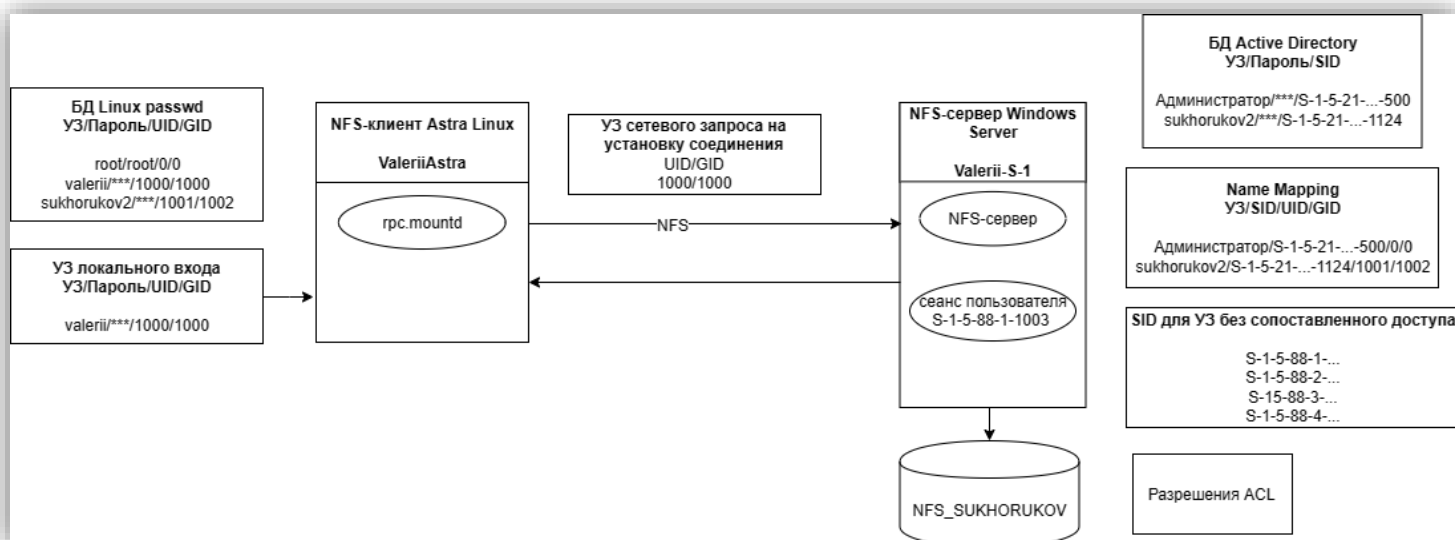


Рис 105.

1. Клиент NFS авторизуется на узле Linux с помощью локальной учетной записи, находящейся в БД passwd.
2. Служба rpc.mountd на клиенте обращается к NFS серверу на узле Windows по протоколу NFS.

3. При обращении к серверу NFS клиент передает UID/GID учетной записи, указанной как параметр подключения (1000/1000).
4. Полученные UID/GID используются для поиска УЗ в БД AD.
5. УЗ с полученными UID/GID не найдена в БД AD. Создается сеанс пользователя с SID S-1-5-88-1-...
6. При наличии разрешения доступа к локальному ресурсу клиенту предоставляется доступ к ресурсу.

7. Использование NFS-клиента на Windows Server.

7.1. Рассмотрим свойства службы “Клиент для NFS”. Стартовать службу. Разберем свойства службы "Клиент для NFS":

❖ **Параметры клиента** - на этой вкладке можно выбрать транспортный протокол, который используется клиентами для подключения к серверам NFS: только UDP, только TCP или TCP+UDP. А также указать тип подключения: мягкое (можно указать количество повторных попыток) или жесткое и интервал между повторными попытками соединения.

❖ **Разрешения для файлов** - на этой вкладке можно указать разрешения, которые будут использоваться клиентами NFS.

❖ **Безопасность** - на этой вкладке можно указать разрешенные флаги безопасности и включить/отключить использование зарезервированных портов.

7.2. Применить NFS-клиент на Windows для монтирования ресурса на NFS-сервере Linux.

Выполним монтирование ресурса от УЗ sukhorukov2 с сопоставленным доступом.

```
C:\Users\sukhorukov2>mount \\192.168.0.108\pub\nfs S:
S: успешно подключен к \\192.168.0.108\pub\nfs
Команда успешно выполнена.
```

Рис 106.

Создадим в подключенном каталоге текстовый файл, и рассмотрим его разрешения. Владелец является УЗ с UID/GID равными 1001/1002 – сопоставление прошло успешно. Установленные разрешения – RWX для владельца, RX для остальных УЗ.

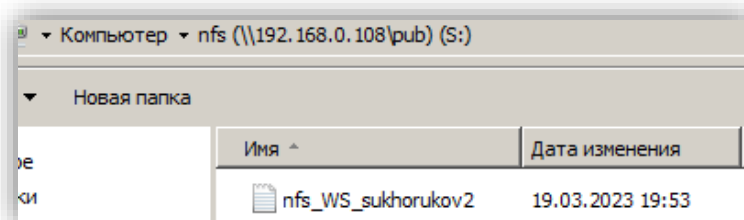


Рис 107.

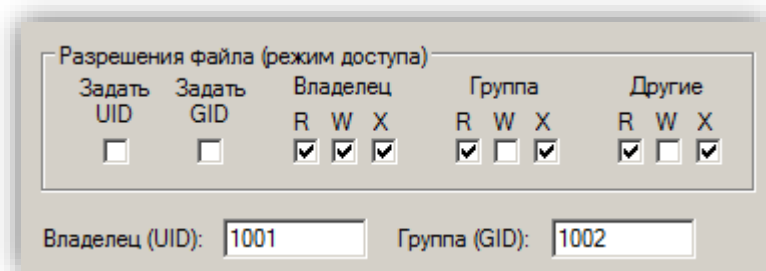


Рис 108.

7.3. Схема сетевого взаимодействия (NFS, Клиент – Windows, Сервер – Linux)

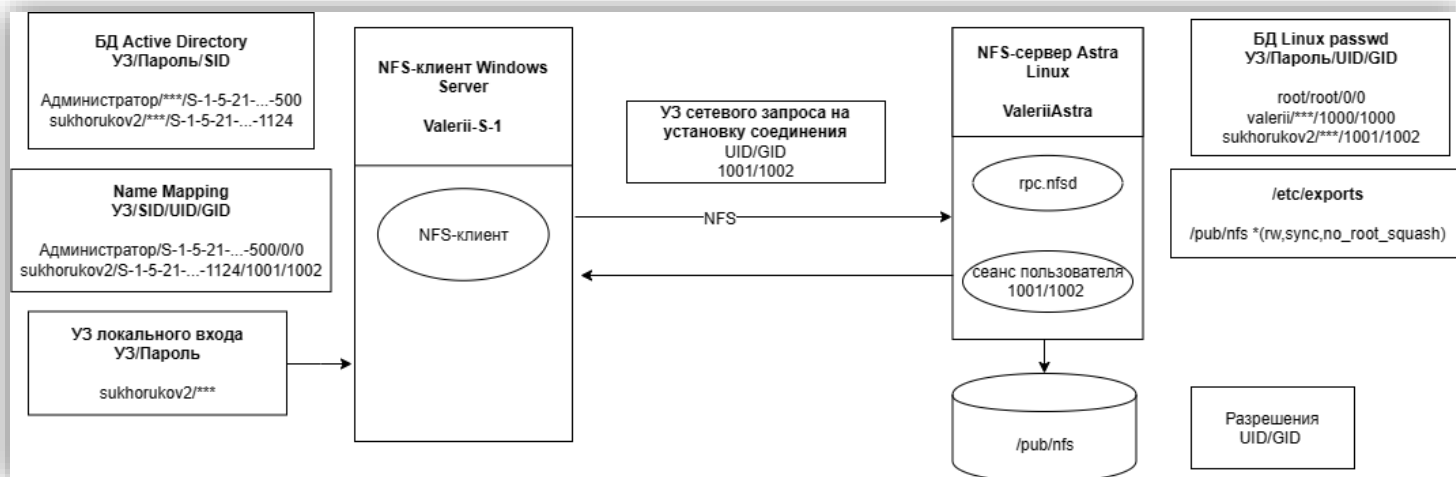


Рис 109.

1. Клиент NFS авторизуется на узле Windows с помощью учетной записи, находящейся в БД AD.
2. Служба NFS-клиент на клиенте Windows обращается к NFS серверу на узле Linux по протоколу NFS.
3. При обращении к серверу NFS клиент передает UID/GID учетной записи, указанной как параметр подключения (1001/1002).
4. Полученные UID/GID сопоставляются с УЗ в БД passwd. Создается сеанс пользователя с uid/gid.
5. При наличии разрешения доступа к сетевому ресурсу в файле /etc/exports клиенту предоставляется доступ к ресурсу. При наличии разрешений к локальному каталогу /pub/nfs разрешается или запрещается та или иная операция.

Вывод

В ходе работы были изучены два протокола для обмена сетевыми файлами – smb и nfs. Данные протоколы различаются по следующим признакам:

NFS был разработан для настройки одним администратором всех компьютеров в локальной сети. На всех компьютерах должны быть созданы нужные УЗ, у которых должны совпадать UID/GID для УЗ с одинаковыми именами.	Для работы SMB нет необходимости создавать весь список локальных УЗ на каждом компьютере. Пользователю необходимо знать имя учетной записи и пароль для доступа с любого компьютера в сети.
В NFS отсутствует механизм аутентификации, т.к. он был разработан для локальной сети.	Аутентификация происходит по имени и паролю учетной записи.
NFS использует систему проверки на основе хоста.	SMB использует систему проверки на основе пользователя
Сервер NFS работает в режиме stateless – не хранит информацию о состоянии подключения.	Сервер SMB работает в режиме statefull – хранит информации о состоянии подключения.
Доступ к каталогу контролируется локальными разрешениями файловой системы.	Устанавливаются сетевые разрешения доступа к каталогам и файлам для УЗ пользователей и групп.