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:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_ Кочешков А. А.\_\_

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Сухоруков В.А.\_\_\_

(подпись) (фамилия, и.,о.)

\_\_\_\_\_\_19-ВМ\_\_\_\_\_\_\_\_

(шифр группы)

Работа защищена «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород 2023

Оглавление

[Цель работы 4](#_Toc130152780)

[Ход работы 4](#_Toc130152781)

[Часть 1. Взаимодействие на базе протокола SMB. 4](#_Toc130152782)

[1. Проверка сетевого доступа по протоколу TCP/IP 4](#_Toc130152783)

[1.1. Получить информацию по настройке сетевых интерфейсов. Сконфигурировать стек по минимальным параметрам. 4](#_Toc130152784)

[1.2. Настроить локальные файлы трансляции DNS-имен. 5](#_Toc130152785)

[2. Реализация сервера файлового доступа SMB на Linux-системе. 7](#_Toc130152786)

[2.1. Ознакомиться с составом Samba. 7](#_Toc130152787)

[2.2. Изучить конфигурирование Samba. 8](#_Toc130152788)

[2.3. Создать учетную запись пользователя Samba. 9](#_Toc130152789)

[2.4. Внутри локального каталога /pub сформировать каталог для выделения в сетевой доступ по smb протоколу 10](#_Toc130152790)

[2.5. Подготовить условия для подключения smb-клиентов и стартовать сервер Samba. 11](#_Toc130152791)

[2.6. В Windows-клиенте проверить доступность и свойства сетевых ресурсов. 11](#_Toc130152792)

[2.7. Схема сетевого взаимодействия (SMB, Клиент –Windows, Cервер - Linux) 16](#_Toc130152793)

[3. Работа SMB-клиента в Linux 17](#_Toc130152794)

[3.1. Использование команды smbclient 17](#_Toc130152795)

[3.2. Использование команды smbtree 18](#_Toc130152796)

[3.3. Использование команды mount.cifs 19](#_Toc130152797)

[3.4. Использование команды smbstatus 20](#_Toc130152798)

[3.5. Схема сетевого взаимодействия (SMB, Клиент –Linux, Cервер - Linux) 21](#_Toc130152799)

[4. Использование команды net. 21](#_Toc130152800)

[2 Часть. Взаимодействие на базе протокола NFS 22](#_Toc130152801)

[5. Сетевая файловая система NFS в Linux. 22](#_Toc130152802)

[5.1. Найти основные компоненты, необходимые для работы NFS 22](#_Toc130152803)

[5.2. Выделение каталога в общий доступ 23](#_Toc130152804)

[5.3. Запуск NFS 24](#_Toc130152805)

[5.4. Монтирование сетевой файловой системы 25](#_Toc130152806)

[5.5. Схема сетевого взаимодействия (NFS, Клиент –Linux, Cервер - Linux) 25](#_Toc130152807)

[6. Использование в Windows Server служб Service for NFS для организации сетевого доступа по протоколу NFS. 26](#_Toc130152808)

[6.1. Настроить файл-сервер в Windows Server 26](#_Toc130152809)

[6.2. Рассмотреть средства согласования учетных записей и свойства службы отображения имен. 26](#_Toc130152810)

[6.3. Служба «Сервер для NFS» 28](#_Toc130152811)

[6.4. На Windows-сервере создать каталог, определить разрешения доступа NTFS. Средствами эксплорера в свойствах каталога настроить параметры экспорта каталога по NFS. 29](#_Toc130152812)

[6.5. На Windows-сервере с помощью консоли администрирования перезапустить сервер NFS. Командой showmount отобразить состояние ресурсов NFS. 29](#_Toc130152813)

[6.6. Схема сетевого взаимодействия (NFS, Клиент –Linux, Cервер – Windows, сопоставленный доступ) 30](#_Toc130152814)

[6.7. Схема сетевого взаимодействия (NFS, Клиент –Linux, Cервер – Windows, несопоставленный доступ) 32](#_Toc130152815)

[7. Использование NFS-клиента на Windows Server. 33](#_Toc130152816)

[7.1. Рассмотреть свойства службы “Клиент для NFS”. Стартовать службу. 33](#_Toc130152817)

[7.2. Применить NFS-клиент на Windows для монтирования ресурса на NFS-сервере Linux. 33](#_Toc130152818)

[7.3. Схема сетевого взаимодействия (NFS, Клиент –Windows, Cервер – Linux) 34](#_Toc130152819)

[Вывод 34](#_Toc130152820)

# Цель работы

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

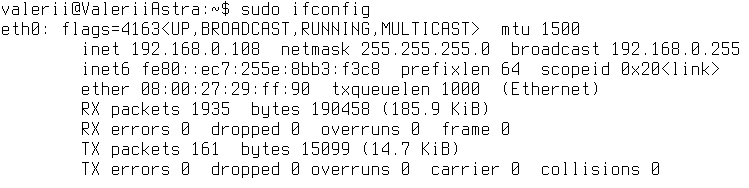
# Ход работы

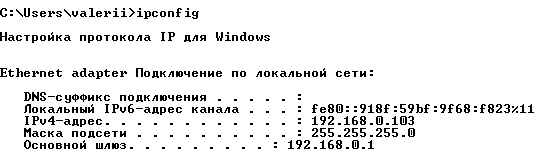
# Часть 1. Взаимодействие на базе протокола SMB.

## Проверка сетевого доступа по протоколу TCP/IP

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

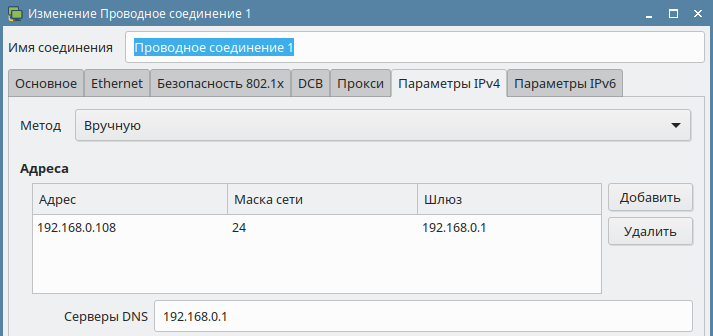
Для соединения двух виртуальных машин в одну сеть установим в свойствах виртуальных машин тип подключения «Сетевой мост». С помощью команд ifconfig для ОС Astra Linux, и ipconfig для ОС Windows 7 получим информацию о настройке сети.



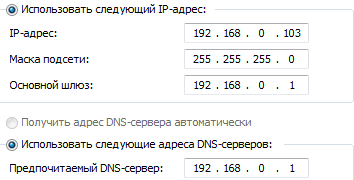


* IP адреса были получены от DHCP сервера.
* Машины находятся в сети 192.168.0.0 с маской сети 255.255.255.0,
* Адрес машины Valerii-Win7 192.168.0.103,
* Адрес машины ValeriiAstra 192.168.0.108

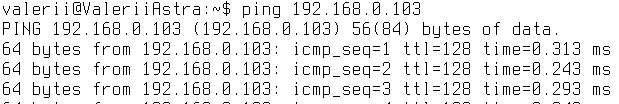
Настроим статические IP адреса на обеих машинах. В свойствах сети на машине ValeriiAstra изменим метод получения IP адреса с «Автоматический (DHCP)» на «Вручную», и установим нужные параметры.



Также настроим сеть на узле Windows.



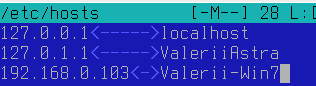
Проверим доступность сети командой ping.



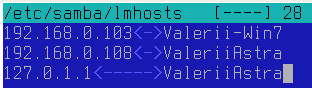
Сеть доступна, и работает корректно.

### Настроить локальные файлы трансляции DNS-имен.

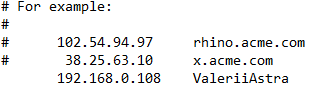
Произведём настройку на узле Linux. Внесем изменения в файл **/etc/hosts**, который содержит информацию о соответствии DNS имен сетевым адресам. Добавим строку с адресом и именем узла Windows.



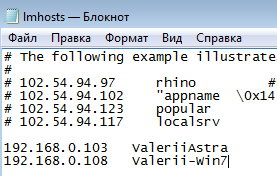
Файл **/etc/samba/lmhosts**, который содержит информацию о соответствии NetBIOS имен сетевым адресам. В текущей версии системы данный файл отсутствует. Создадим его, и добавим строки с адреса и именами узлов Windows и Linux.



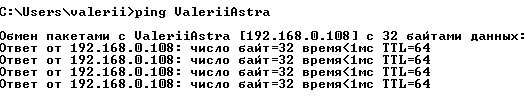
Произведём настройку на узле Windows. В файл **%SYSTEMROOT%\system32\drivers\etc\hosts** запишем соответствие DNS имени и ip-адреса хоста на Linux машине.

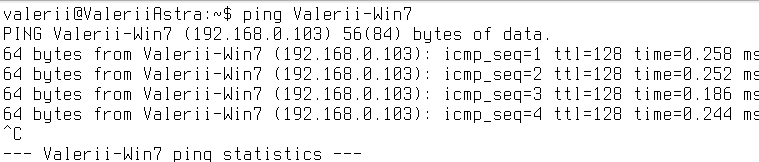


В файл **%SYSTEMROOT%\system32\drivers\etc\lmhosts.asm** запишем соответствие NetBIOS имени и ip-адреса хоста на Linux и Windows машинах.



Проверим доступность узлов указав в команде ping DNS адреса узлов.





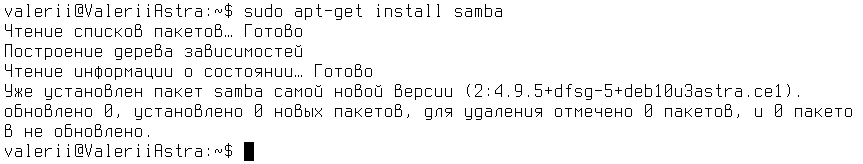
Доступ по сети через DNS адреса возможен. Сеть настроена корректно.

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

### 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**



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



**/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-proxy
* 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





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













### 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:

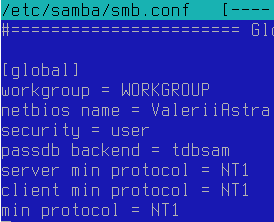
* workgroup - Определяет, в какой рабочей группе будет находиться сервер.
* NetBIOS name - Устанавливает NetBIOS-имя Samba-сервера. По умолчанию оно совпадает с первым компонентом DNS-имени хоста.
* security- определяет режим безопасности в соответствии с механизмом аутентификации SMB. Режим доступа 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

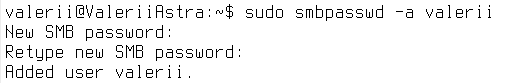
passdb bachend = tdbsam

Разрешим использовать версию протокола SMB1.

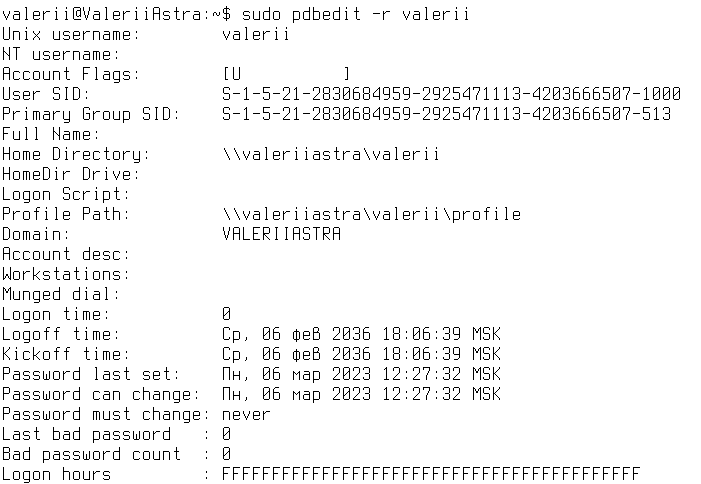


### Создать учетную запись пользователя Samba.

Создадим учетную запись пользователя Samba. Для этого используем команду smbpasswd с ключом –а.



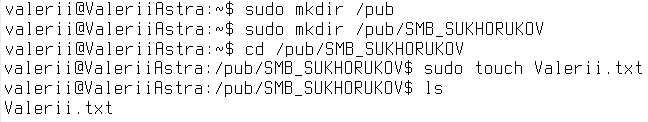
Получим информацию об учетной записи командой pdbedit.



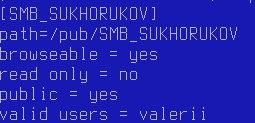
При применении ключа –r в команде pdbedit возможно просмотреть множество параметров учетной записи в БД samba, например, SID пользователя, время последней смены пароля и т.д.

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

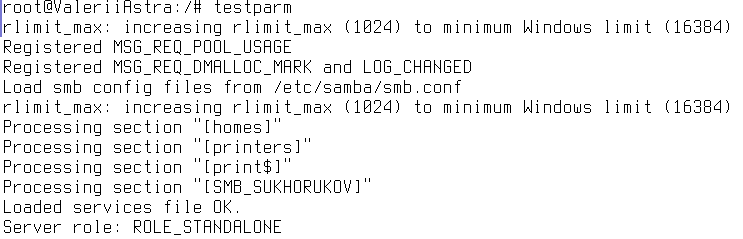
Создадим локальный каталог /pub внутри которого сформируем каталог "SMB\_SUKHORUKOV". В последнем создадим текстовый файл "Valerii.txt".

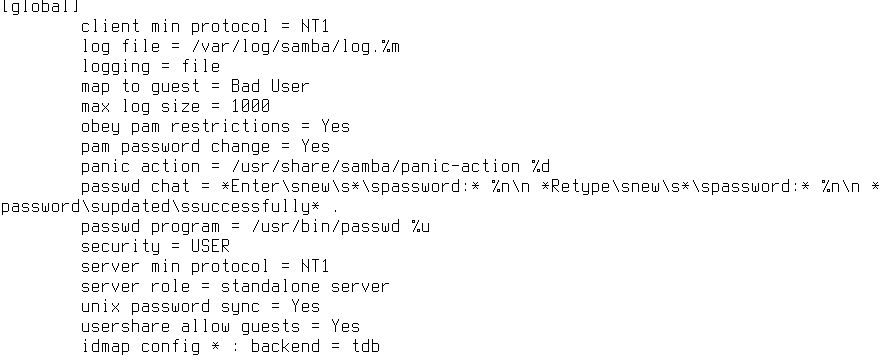


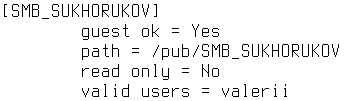
Теперь внесем созданный сетевой ресурс " SMB\_SUKHORUKOV " со следующими параметрами в файл smb.conf



Проверим корректность конфигурации командой testparm. Параметры секции [global] и секции [SMB\_SUKHORUKOV] применились корректно.

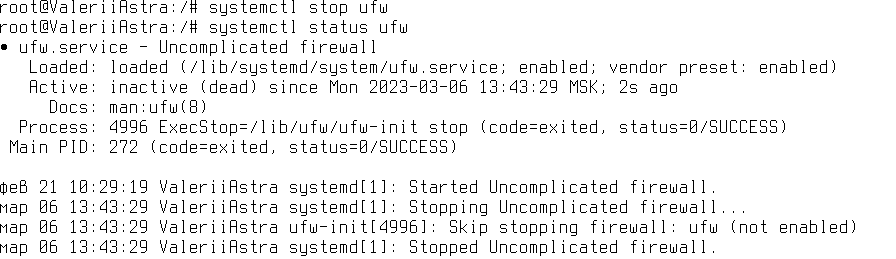






### Подготовить условия для подключения smb-клиентов и стартовать сервер Samba.

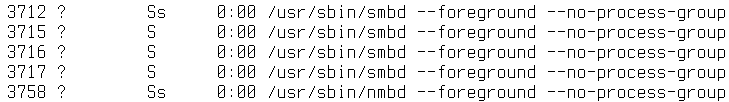
Отключим межсетевой экран командой **systemclt stop ufw**, и проверим его состояние командой **systemclt status ufw**. Межсетевой экран успешно отключился.



Запустим сервер Samba.



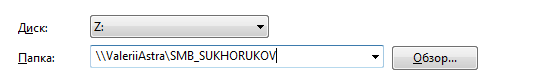
В списке процессов найдем нужные процессе-демоны, используя команду **ps –x**. Демоны smdb и nmdb успешно запустились.



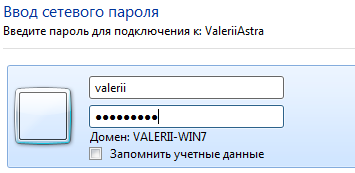
### В Windows-клиенте проверить доступность и свойства сетевых ресурсов.

#### Подключение ресурса

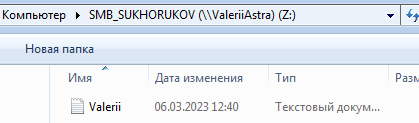
Чтобы проверить доступность нашего созданного сетевого ресурса попробуем подключить сетевой диск. Обратимся к Linux узлу по NetBIOS имени.



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



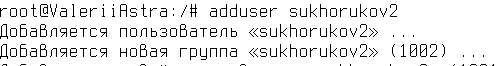
Результатом успешных настроек двух узлов является доступ к сетевому ресурсу.



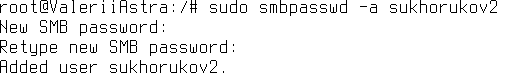
#### Проверка прав на подключение

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

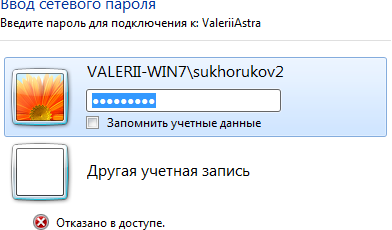
Создадим локальную учетную запись пользователя командой adduser.



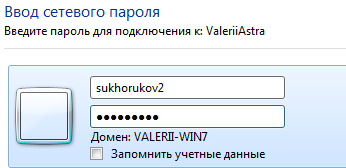
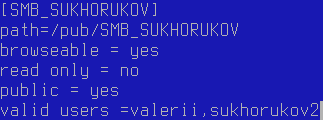
Создадим учетную запись Samba с таким же именем.



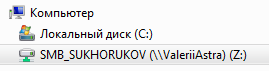
Попробуем подключиться к ресурсу, явно указав данные новой учетной записи.



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.

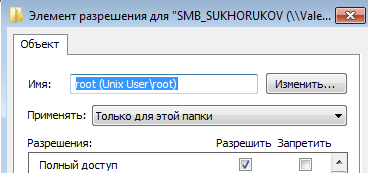
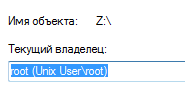


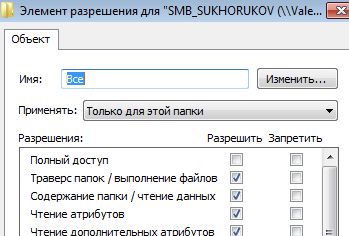
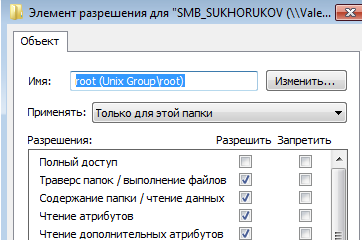
После добавления учетной записи в список разрешённых, удалось получить доступ с помощью неё.



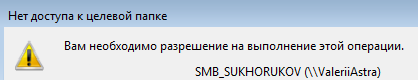
#### Разрешения доступа к каталогу

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.

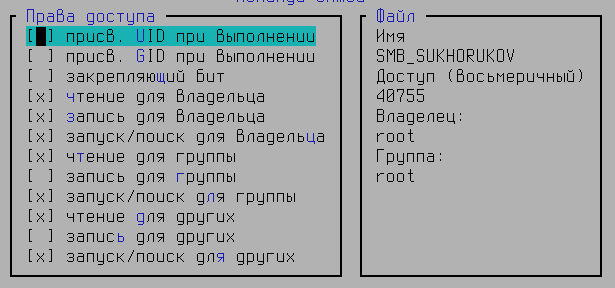




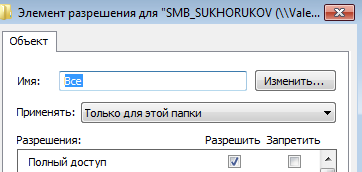
При выделении каталога в общий доступ параметру «read only» было присвоено значение «no», однако доступ к каталогу доступен только по чтению, при попытке создать файл внутри подключенного каталога возникает ошибка.



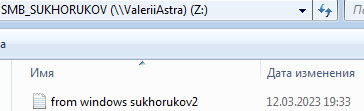
Посмотрим локальные разрешения каталога на узле Linux.

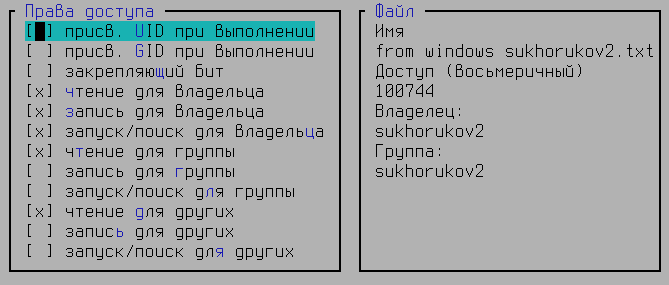


Для владельца root установлены разрешения полного доступа, для других пользователей установлены разрешения на чтения. Установим разрешение на «запись для других». После этого на узле Windows изменилось отображение прав для группы «Все» (Рис 40).



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

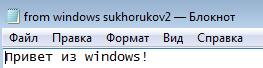




Владельцем файла является учетная запись sukhorukov2. У данной учетной записи полный доступ к файлу, у других только на чтение.

#### Проверка отображения содержимого

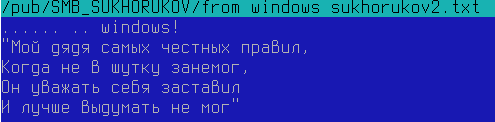
Запишем в файл информацию на русском и английском языке.



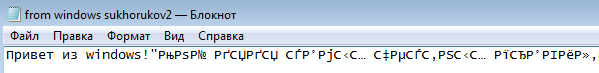
На Linux узле русский текст отображается некорректно из-за использования разных кодировок на разных ОС.



На Linux изменим файл, добавив новые строки.

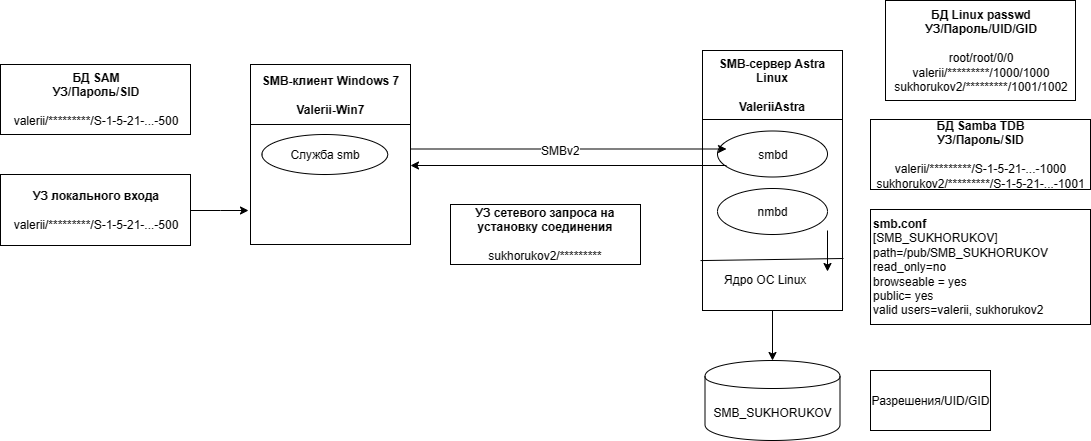


На Windows узле просмотрим содержимое файла. Русский язык также отображается некорректно, и содержимое файла представляется одной строкой. Это связано с разной кодировкой переноса строки на Windows и Linux.



### Схема сетевого взаимодействия (SMB, Клиент –Windows, Cервер - Linux)

Составим схему сетевого взаимодействия узлов.

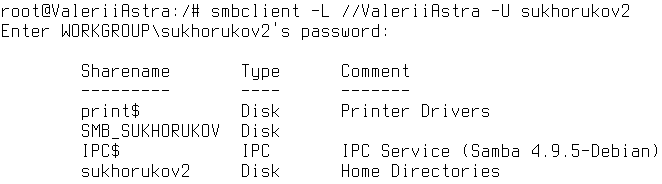


1. Клиент SMB авторизуется на узле Windows с помощью локальной учетной записи, находящейся в БД SAM.
2. При обращении к серверу SMB клиент авторизуется с помощью УЗ, находящейся в БД Samba на сервере.
3. Служба smb на клиенте обращается к процессу smbd на сервере по протоколу SMBv2.
4. Демон smbd сопоставляет 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.

## Работа SMB-клиента в Linux

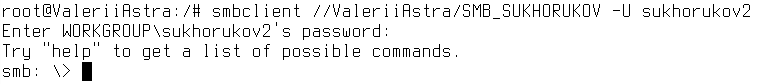
### Использование команды smbclient

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



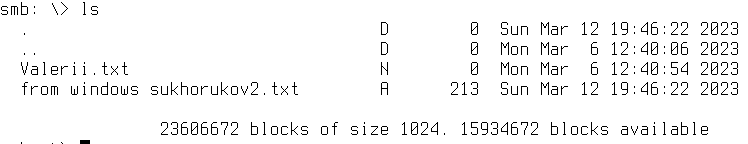
* Print$ - используется для общего доступа к принтерам в рабочей группе.
* SMB\_SUKHORUKOV – созданный ресурс.
* IPC$ - используется при организации временных подключений, создаваемых приложениями для обмена данными с помощью именованных каналов.
* sukhorukov2 – домашний каталог пользователя на узле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

Подключимся с помощью данной утилиты к ресурсу SMB\_SUKHORUKOV.



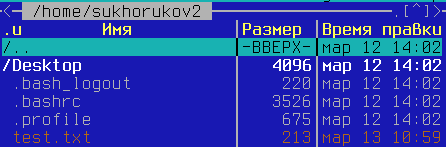
После подключения можно выполнять разовые отладочные действия с каталогом. Опробуем на практике основные команды:

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

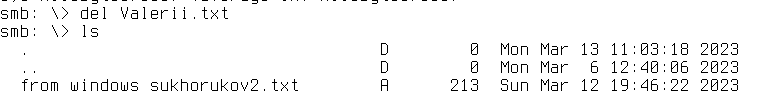


* get- копирует файл с сервера. Скопируем текстовый файл "from windows sukhorukov2", который был создан на Windows машине, в домашний каталог пользователя.

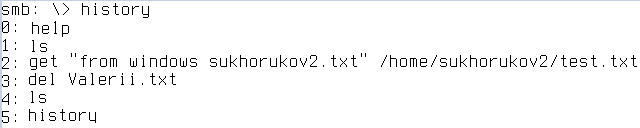




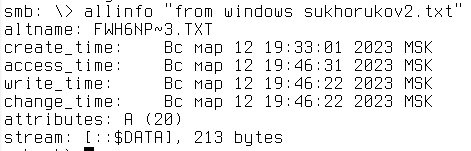
* del- удаление файла с сервера. Удалим текстовый файл "valerii.txt".



* history- выводит историю выполнения команд.



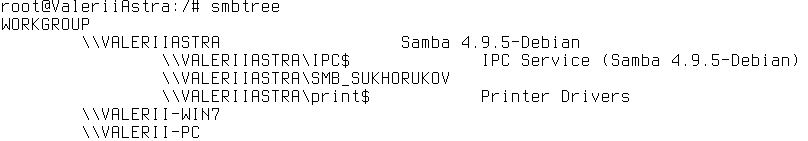
* allinfo- выводит всю информацию о файле или каталоге.



### 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.

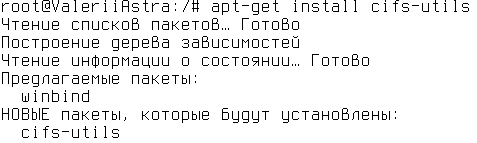
С помощью команды smbtree выполним обзор smb-ресурсов.



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].

### Использование команды mount.cifs

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



Выполним монтирование каталога SMB\_SUKHORUKOV в каталог /mnt/smb

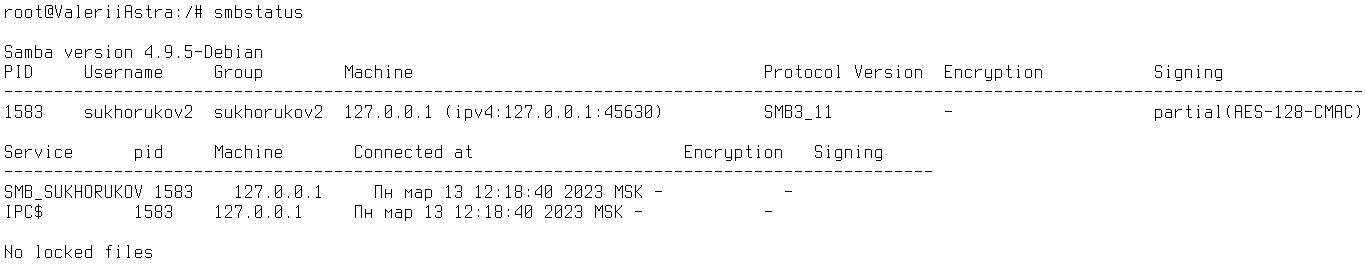


Подключенный ресурс успешно подключился.



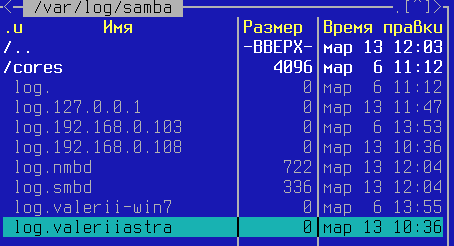
### Использование команды smbstatus

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

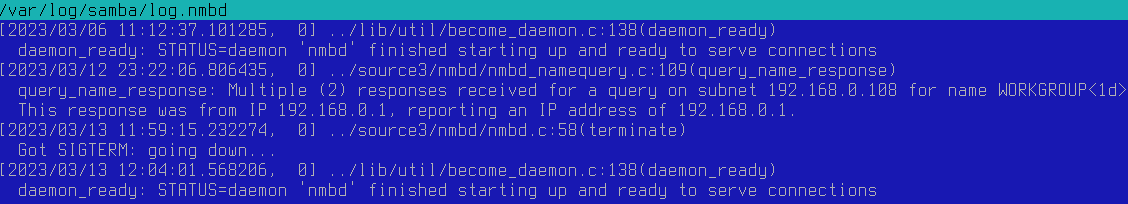


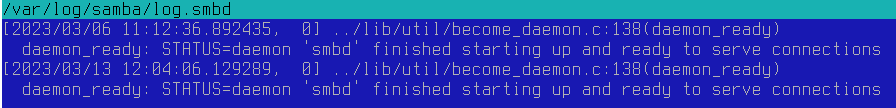
Результатом выполнения является список учетных записей пользователей, IP адресов машин, с которой произошло подключение, и список используемых сетевых ресурсов.

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

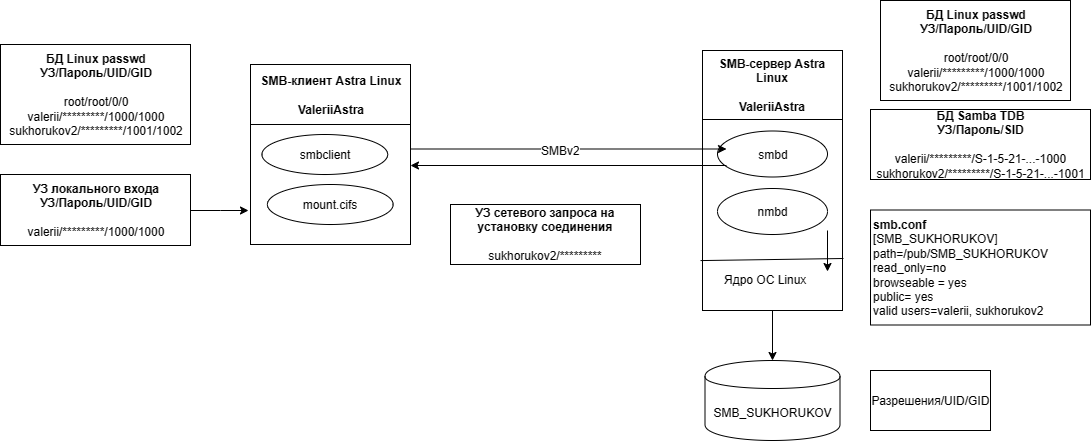


log.smbd и log.nmbd содержат информация о включении/выключении nmbd и smbd демонов. Также в файле log.nmbd содержатся сообщения, связанные с функционалом Samba NETBIOS over IP, в log.smbd - сообщения, связанные с функционалом Samba SMB/CIFS.





### Схема сетевого взаимодействия (SMB, Клиент –Linux, Cервер - Linux)



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 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.

## 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:

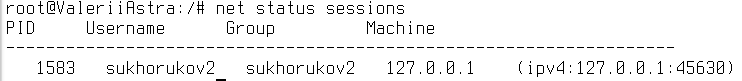
* net getlocalsid- позволяет получить SID данного сервера.



* net lookup имя\_хоста- позволяет узнать по имени хоста его IP-адрес.



* net status sessions- выводит информацию о сессиях.



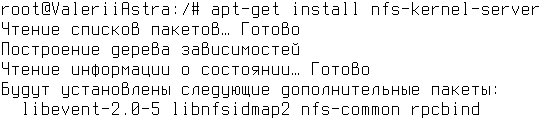
# 2 Часть. Взаимодействие на базе протокола NFS

## Сетевая файловая система NFS в Linux.

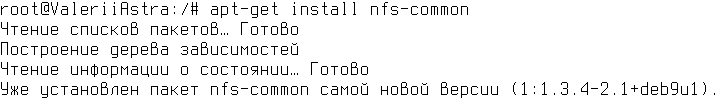
### Найти основные компоненты, необходимые для работы NFS

*Network File System (NFS)* — [протокол сетевого доступа](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) к [файловым системам](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0), первоначально разработан [Sun Microsystems](https://ru.wikipedia.org/wiki/Sun_Microsystems) в [1984 году](https://ru.wikipedia.org/wiki/1984_%D0%B3%D0%BE%D0%B4). За основу взят протокол вызова удалённых процедур ([ONC RPC](https://ru.wikipedia.org/wiki/ONC_RPC), [англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) 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**



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



Клиентская часть установилась вместе с серверной.

Рассмотрим основные компоненты nfs.

**/etc/…**

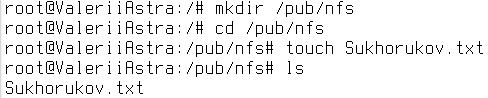
* exports - Конфигурационный файл nfs, содержит список экспортируемых файловых систем.
* nfsmount.conf - Конфигурационный файл, позволяет установить опции монтирования глобально, для каждого сервера или для каждой точки монтирования.
* mtab - содержат информацию о смонтированных файловых системах

**/usr/sbin/…**

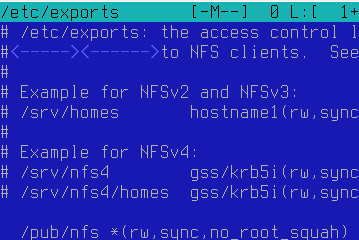
* rpc.nfsd - Основной процесс NFS сервера.
* rpc.mountd - NFS демон монтирования.
* rpc.statd - Демон мониторинга статуса хостов.
* rpcbind (portmapper) - Утилита, конвертирующая RPC номер программы в универсальный адрес.
* rpcinfo – Утилита получения информации о RPC
* exportfs - Утилита, обслуживающая таблицу экспортированных NFS файловых систем.

### Выделение каталога в общий доступ

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



Опишем экспорт каталога в **/**etc/exports.



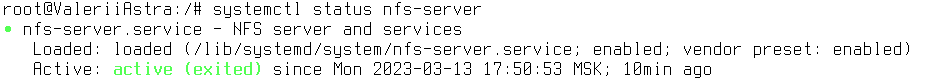
К каталогу можно подключиться с помощью любой учетной записи. Доступ предоставлен по чтению и по записи. Опция no\_root\_squashиспользуется для доступа root по сети.

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.



### Запуск NFS

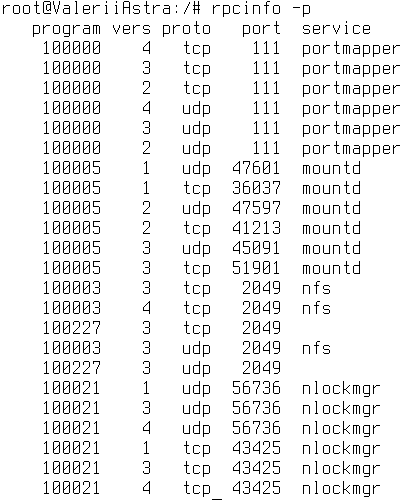
Перезапустим демоны NFS командой **systemclt restart nfs-serve**r. Проверим статус командой **systemclt status nfs-serve**r.



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



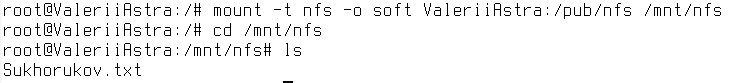
Определим протоколы и порты сервисов NFS командой **rpcinfo –p**.



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

### Монтирование сетевой файловой системы

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



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

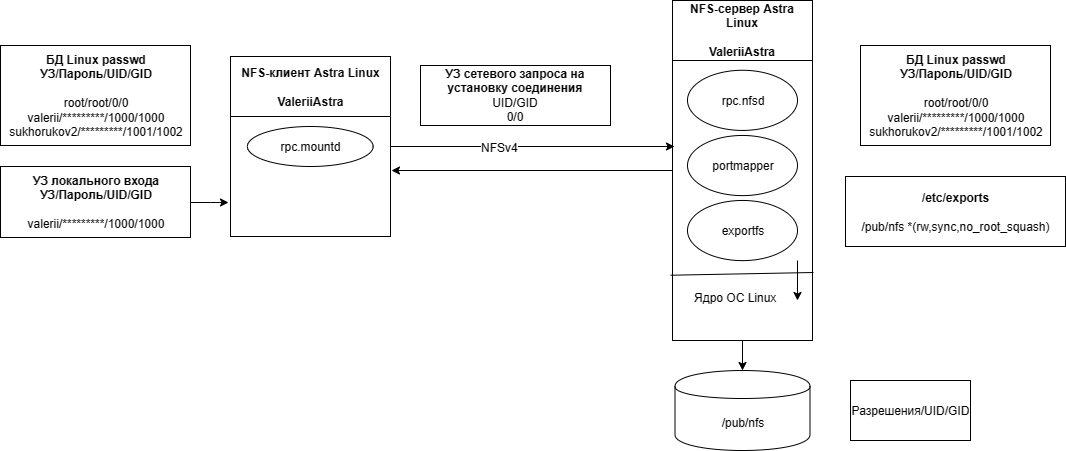


Можно увидеть, что при монтировании был использован протокол NFS4.

Размонтируем подключенный ресурс командой **umount**.



### Схема сетевого взаимодействия (NFS, Клиент –Linux, Cервер - Linux)

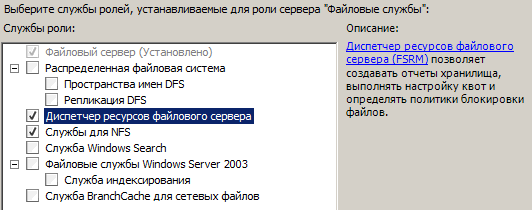


1. Клиент NFS авторизуется на узле Linux с помощью локальной учетной записи, находящейся в БД passwd.
2. Служба rpc.mountd на клиенте обращается к процессу rpc.nfsd на сервере по протоколу NFSv4.
3. При обращении к серверу NFS клиент авторизуется с помощью УЗ, находящейся в БД passwd на сервере.
4. Полученные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

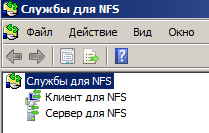
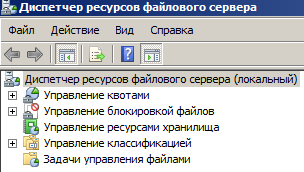
## Использование в Windows Server служб Service for NFS для организации сетевого доступа по протоколу NFS.

### 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».



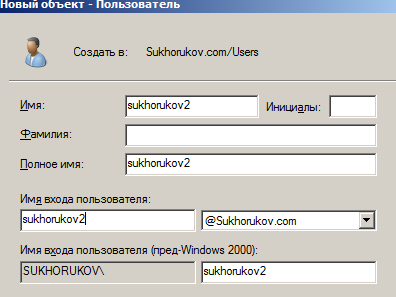
После установки в меню "Администрирование" появились оснастки "Диспетчер ресурсов файлового сервера" и "Службы для NFS".



### 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.

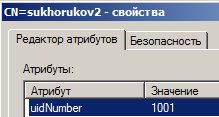
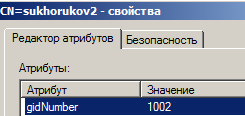
Создадим в БД AD на контроллере домена в Windows учетную запись с именем sukhorukov2, как на узле Windows.



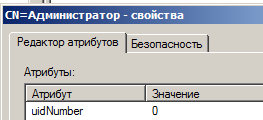
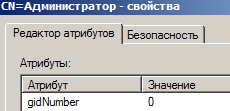
Получим UID, GID УЗ в Linux с помощью команды **id**.



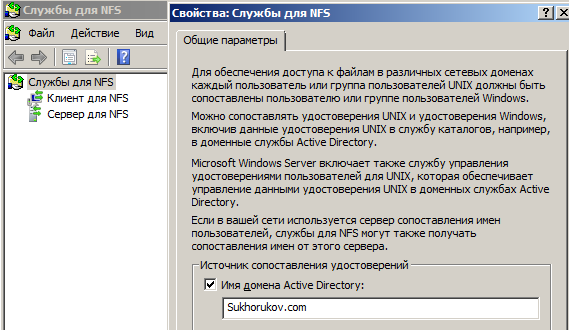
С помощью оснастки «Редактирование ADSI» настроим согласование учетных записей.



Также установим согласование УЗ «Администратор» с УЗ root, указав uidNUmber и gidNUmber равные 0.



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

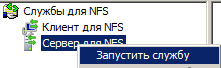


### Служба «Сервер для NFS»

Разберем свойства службы "Сервер для NFS":

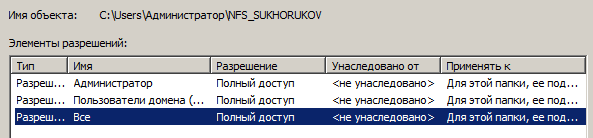
* **Параметры сервера**- на этой вкладке можно включить/отключить поддержку NFS 3 версии, выбрать транспортный протокол: только UPD, только TCP или TCP+UDP. Также можно задать периодическую проверку данных подлинности пользователей или же вообще ее не выполнять.
* **Обработка имен файлов**- на этой вкладке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

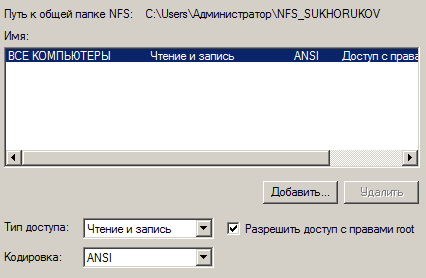
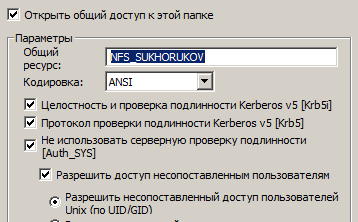


### На Windows-сервере создать каталог, определить разрешения доступа NTFS. Средствами эксплорера в свойствах каталога настроить параметры экспорта каталога по NFS.

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



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

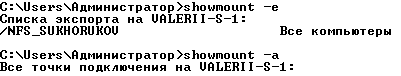


### На Windows-сервере с помощью консоли администрирования перезапустить сервер NFS. Командой showmount отобразить состояние ресурсов NFS.

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

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

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



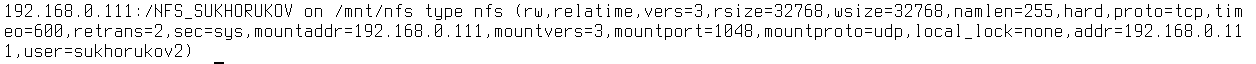
Так как мы еще не смонтировали наш файловый ресурс, поэтому мы не видим клиентов NFS, которые отображаются командой showmount -а.

### Схема сетевого взаимодействия (NFS, Клиент –Linux, Cервер – Windows, сопоставленный доступ)

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



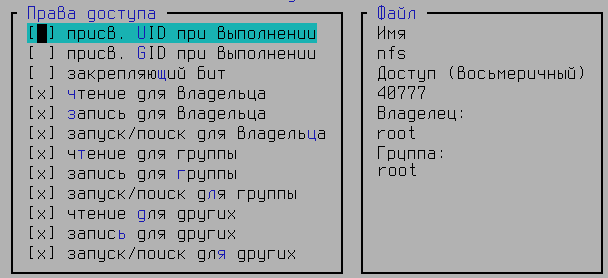
Командой mount без параметров получим список смонтированных файловых систем, и найдём смонтированный каталог.



Проверим командой showmount -а точки подключения на узле Windows.

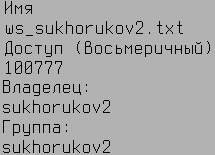
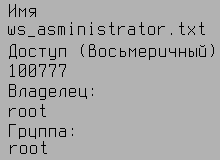


Каталог успешно смонтировался. Просмотрим права доступа у подключённого каталога.

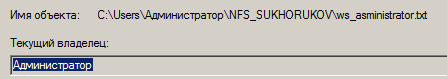


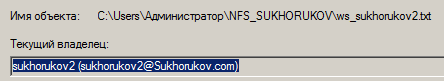
Учетная запись «Администратор» сопоставилась с УЗ «root».

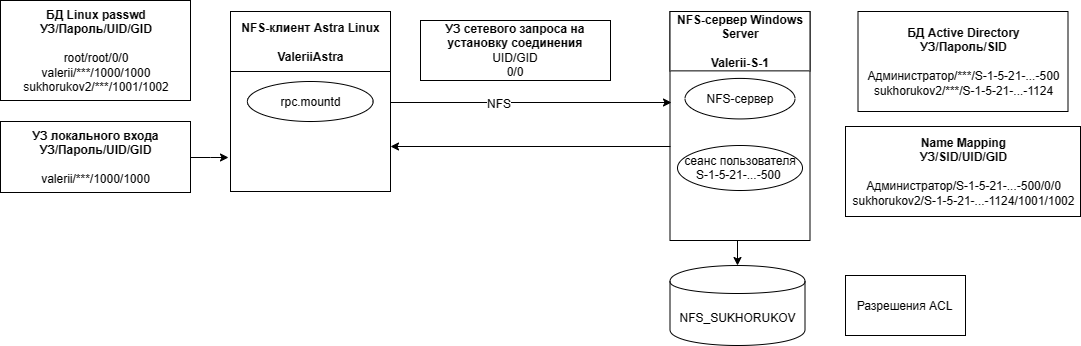
Создадим на узле Linux два файла, используя разные учетные записи – root, и sukhorukov2.



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







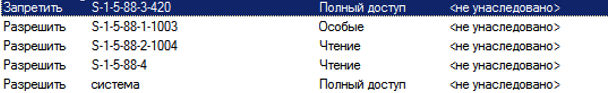
1. Клиент NFS авторизуется на узле Linux с помощью локальной учетной записи, находящейся в БД passwd.
2. Служба rpc.mountd на клиенте обращается к NFS серверу на узле Windows по протоколу NFS.
3. При обращении к серверу NFS клиент передает UID/GID учетной записи, указанной как параметр подключения (0/0).
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.

### Схема сетевого взаимодействия (NFS, Клиент –Linux, Cервер – 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.

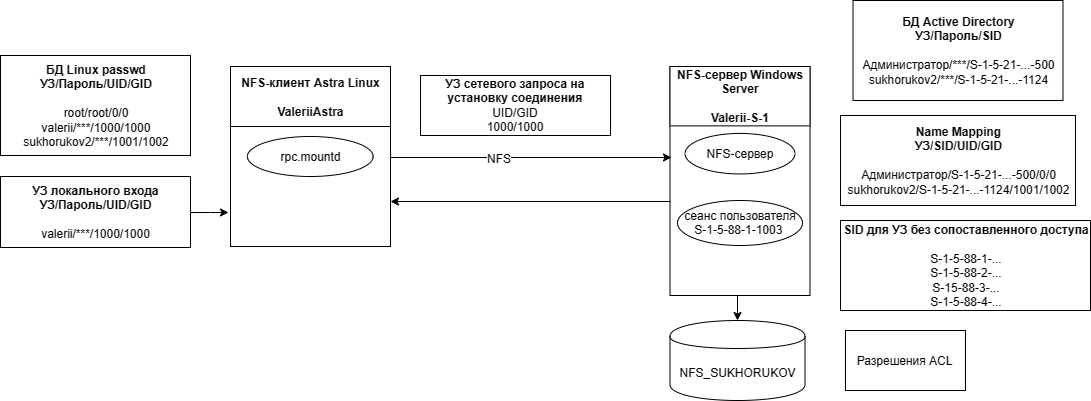


Создадим в подключенном каталоге файл и просмотрим его разрешения на Windows-сервере.



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.



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.

## Использование NFS-клиента на Windows Server.

### Рассмотреть свойства службы “Клиент для NFS”. Стартовать службу.

Разберем свойства службы "Клиент для NFS":

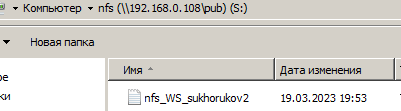
* **Параметры клиента** - на этой вкладке можно выбрать транспортный протокол, который используется клиентов для подключения к серверам NFS: только UPD, только TCP или TCP+UDP. А также указать тип подключения: мягкое (можно указать количество повторных попыток) или жесткое и интервал между повторными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

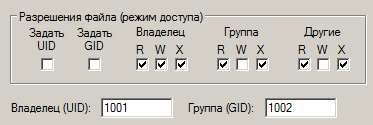
### Применить NFS-клиент на Windows для монтирования ресурса на NFS-сервере Linux.

Выполним монтирование ресурса от УЗ sukhorukov2 с сопоставленным доступом.

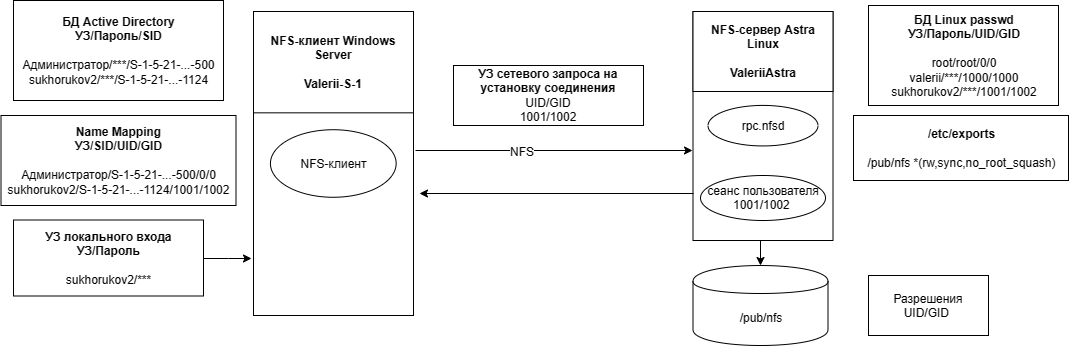


Создадим в подключенном каталоге текстовый файл, и рассмотрим его разрешения. Владельцем является УЗ с UID/GID равными 1001/1002 – сопоставление прошло успешно. Установленные разрешения – RWX для владельца, RX для остальных УЗ.





### Схема сетевого взаимодействия (NFS, Клиент –Windows, Cервер – Linux)



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. |