



**Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)**

ФАКУЛЬТЕТ Информатика и системы управления

КАФЕДРА Системы обработки информации и управления

Отчет по лабораторной работе № 4

**«Сетевая файловая система NFS.
Установка и настройка сервера и клиентов файловой системы»
по дисциплине «Сетевое программное обеспечение»**

Студент ИУ5-61Б
(Группа)

Е.И. Бирюкова
(Подпись, дата) (И.О.Фамилия)

Преподаватель

П.С. Семкин
(Подпись, дата) (И.О.Фамилия)

Москва

2025

Цель работы

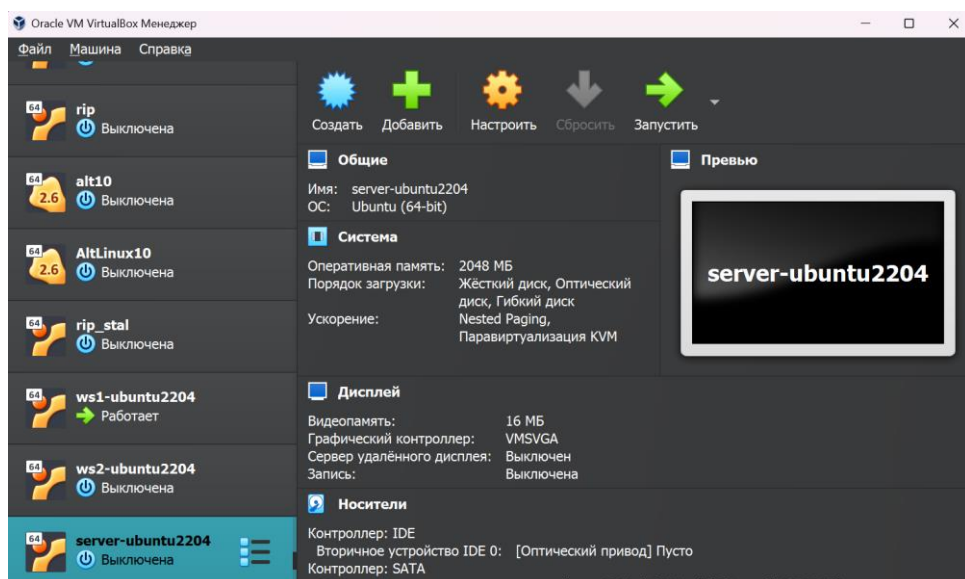
Целью работы является получение навыков по установке и настройке файлового сервера и клиентов NFS для работы в локальной сети Ubuntu.

Задание

1. Установить на сервере server-ubuntu2204 программу сервера файловой системы NFS.
2. Создать на сервере server-ubuntu2204 пользователя-администратора NFS.
3. Создать разделяемые каталоги и файлы NFS, установить владельца, группу и права доступа к каталогам.
4. Настроить файловый сервер NFS с помощью редактирования файла конфигурации и с использованием программы удалённого администрирования Webmin.
5. Установить на рабочей станции ws1-ubuntu программу клиента файловой системы NFS.
6. Смонтировать каталоги NFS в точки монтирования на рабочей станции с использованием статического монтирования и автосмонтирования.

Порядок выполнения работы

1. Войти в систему под учётной записью stud_XX пароль studXX
2. Запустить программу виртуализации VirtualBox

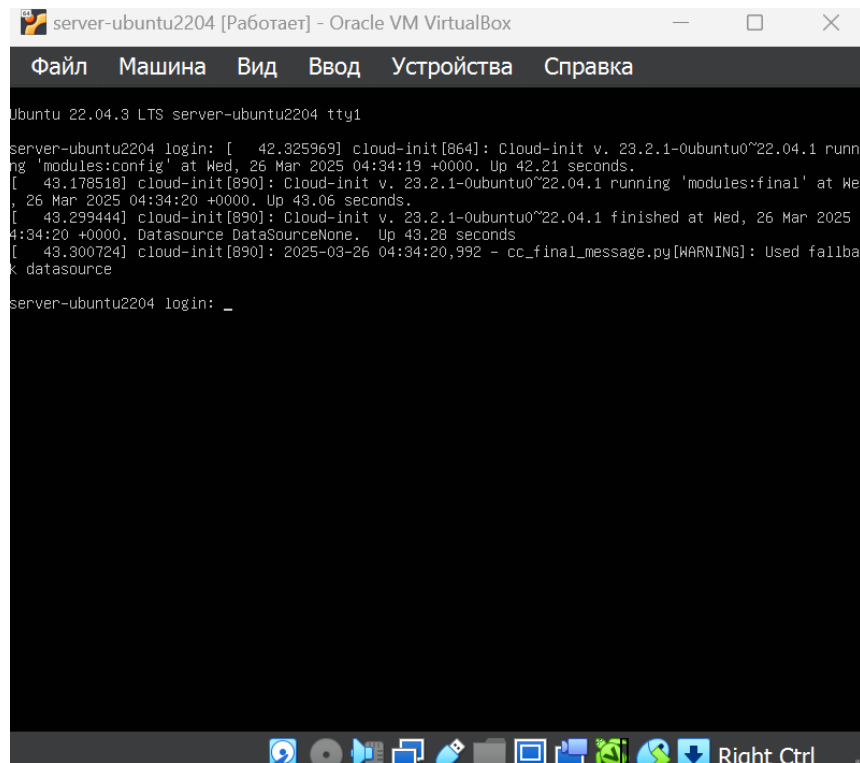


3. Запустить виртуальные машины сервера и рабочей станции

3.1. Запустить виртуальную машину server-ubuntu2204 (с установленной операционной системой Ubuntu Server 22.04.3 LTS и настроенными программой Webmin и сетевыми интерфейсами).

Логин – admin_server

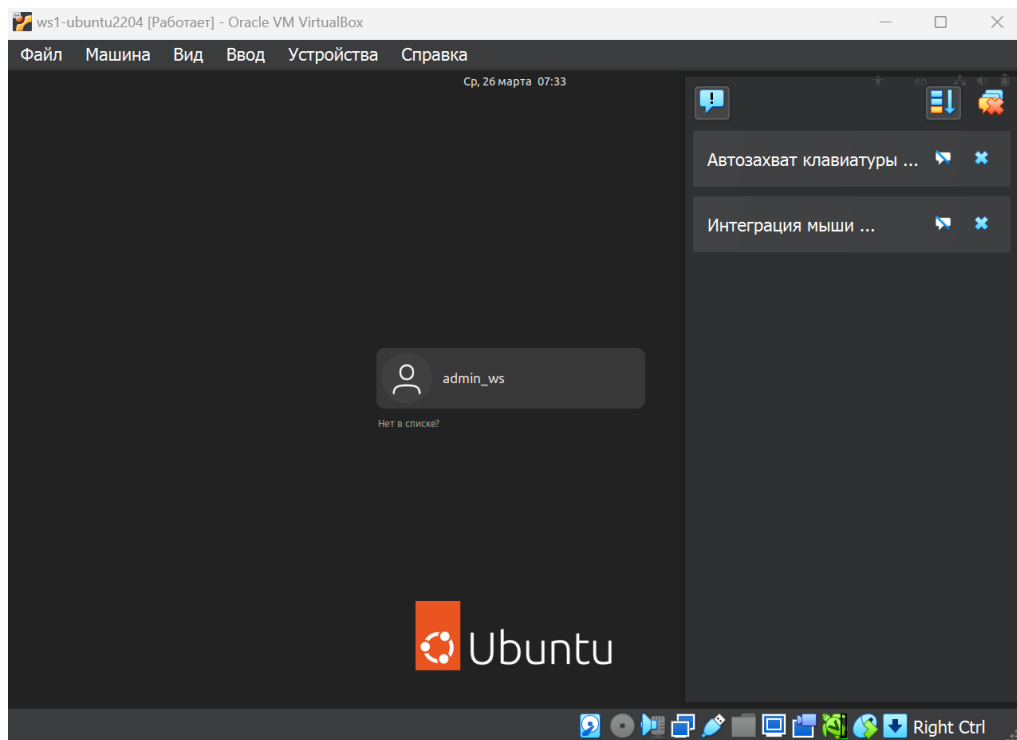
Пароль – adminserver



3.2. Запустить виртуальную машину ws1-ubuntu2204 (с установленной операционной системой Ubuntu 22.04.3 LTS и настроенными сетевыми интерфейсами)

Логин - admin_ws

Пароль – adminws



4. Установить сервер файловой системы NFS

4.1. перейти на виртуальную машину server-ubuntu2204

```
server-ubuntu2204 login: [ 42.325969] cloud-init[864]: Cloud-init v. 23.2.1-0ubuntu0~22.04.1 running 'modules:config' at Wed, 26 Mar 2025 04:34:19 +0000. Up 42.21 seconds.
[ 43.178518] cloud-init[890]: Cloud-init v. 23.2.1-0ubuntu0~22.04.1 running 'modules:final' at Wed, 26 Mar 2025 04:34:20 +0000. Up 43.06 seconds.
[ 43.299444] cloud-init[890]: Cloud-init v. 23.2.1-0ubuntu0~22.04.1 finished at Wed, 26 Mar 2025 04:34:20 +0000. Datasource DataSourceNone. Up 43.28 seconds
[ 43.300724] cloud-init[890]: 2025-03-26 04:34:20,992 - cc_final_message.py[WARNING]: Used fallback datasource

server-ubuntu2204 login: admin_server
Password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-94-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Cp 26 map 2025 04:35:42 UTC

System load:  0.66357421875   Processes:            109
Usage of /:   48.9% of 11.21GB Users logged in:      0
Memory usage: 14%            IPv4 address for enp0s3: 10.0.2.15
Swap usage:   0%             IPv4 address for enp0s8: 192.168.100.100

Expanded Security Maintenance for Applications is not enabled.

218 updates can be applied immediately.
114 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Wed Mar 12 07:31:49 UTC 2025 on tty1
admin_server@server-ubuntu2204:~$
```

4.2. Выполнить команды установки пакета сервера NFS

```
admin_server@server-ubuntu2204:~$ sudo apt-get update_
...
admin_server@server-ubuntu2204:~$ sudo apt-get install nfs-kernel-server
Reading package lists... Done
```

4.3. Проверить использование порта сервером NFS (соединения NFS, как для TCP, так и для UDP, используют порт 2049)

```
admin_server@server-ubuntu2204:~$ rpcinfo -p | grep nfs
100003      3      tcp    2049    nfs
100003      4      tcp    2049    nfs
admin_server@server-ubuntu2204:~$
```

4.4. Проверить поддержку NFS на уровне ядра

```
admin_server@server-ubuntu2204:~$ cat /proc/filesystems | grep nfs
nodev      nfsd
```

4.5. Добавить запуск сервера NFS в автозагрузку

```
admin_server@server-ubuntu2204:~$ sudo systemctl enable nfs-server_
```

5. Создать пользователя сервера NFS

5.1. Перейти на виртуальную машину server-ubuntu2204

```
100003      3      tcp    2049    nfs
100003      4      tcp    2049    nfs
admin_server@server-ubuntu2204:~$ [ 746.225747] watchdog: BUG: soft lockup - CPU#0 stuck for 299s!
[swapper/0:0]
[ 746.255913] systemd[1]: systemd-logind.service: Watchdog timeout (limit 3min)!
[ 746.280600] systemd[1]: snapd.service: Watchdog timeout (limit 5min)!

admin_server@server-ubuntu2204:~$
admin_server@server-ubuntu2204:~$
admin_server@server-ubuntu2204:~$ cat /proc/filesystems | grep nfs
nodev      nfsd
admin_server@server-ubuntu2204:~$ sudo systemctl enable nfs-server
admin_server@server-ubuntu2204:~$
```

5.2. Создать нового пользователя на сервере server-ubuntu2204

admin_nfs/adminnfs

```
admin_server@server-ubuntu2204:~$
admin_server@server-ubuntu2204:~$ sudo adduser admin_nfs_
```

```
admin_server@server-ubuntu2204:~$ sudo usermod -aG sudo admin_nfs
admin_server@server-ubuntu2204:~$ _
```

6. Создать каталоги NFS и установить владельца, группы и права доступа для каталога

6.1. Создать каталоги общего доступа в каталоге NFS

/ nfs / share_nfs

/ nfs / sharer_nfs

```
admin_server@server-ubuntu2204:~$ sudo mkdir -p /nfs/share_nfs
admin_server@server-ubuntu2204:~$ sudo mkdir -p /nfs/sharer_nfs
```

6.2. Создать файл общего доступа в каталоге NFS

/ nfs /share_nfs / file_nfs

```
admin_server@server-ubuntu2204:~$ sudo mkdir -p /nfs/share_nfs
admin_server@server-ubuntu2204:~$ sudo touch /nfs/share_nfs/file_nfs
```

6.3. Назначить владельца и группу каталога NFS. Назначить владельцем каталога / nfs пользователя admin_nfs. Группой назначить группу admin_nfs

```
admin_server@server-ubuntu2204:~$ sudo touch /nfs/share_nfs/file_nfs
admin_server@server-ubuntu2204:~$ sudo chown -R admin_nfs:admin_nfs /nfs/
admin_server@server-ubuntu2204:~$
```

6.4. Установить права доступа к каталогу NFS

```
admin_server@server-ubuntu2204:~$ sudo chmod -R 0777 /nfs
admin_server@server-ubuntu2204:~$
```

6.5. Проверить созданные каталоги

```
admin_server@server-ubuntu2204:~$ ls -la /nfs
total 16
drwxrwxrwx  4 admin_nfs admin_nfs 4096 map 26 05:00 .
drwxr-xr-x 21 root      root      4096 map 26 05:00 ..
drwxrwxrwx  2 admin_nfs admin_nfs 4096 map 26 05:02 share_nfs
drwxrwxrwx  2 admin_nfs admin_nfs 4096 map 26 05:00 sharer_nfs
admin_server@server-ubuntu2204:~$ ls -la /nfs/share_nfs
total 8
drwxrwxrwx 2 admin_nfs admin_nfs 4096 map 26 05:02 .
drwxrwxrwx 4 admin_nfs admin_nfs 4096 map 26 05:00 ..
-rwxrwxrwx 1 admin_nfs admin_nfs   0 map 26 05:02 file_nfs
```

7. Настроить сервер NFS с помощью редактирования файла конфигурации

7.1. Необходимо настроить общий доступ к каталогу / nfs /share_nfs для всех пользователей с возможностью чтения и записи.

```
admin_server@server-ubuntu2204:~$ sudo nano /etc/exports_
```

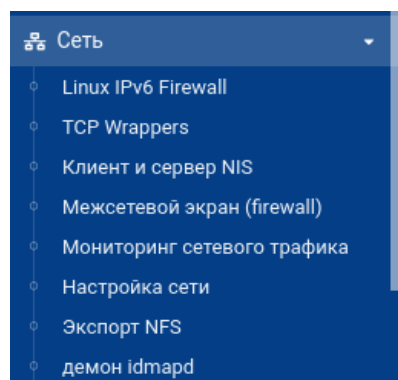
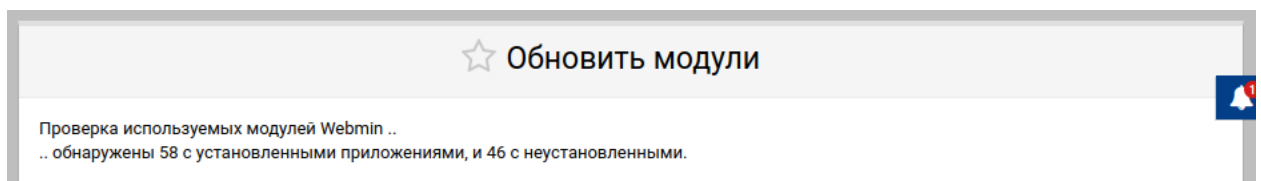
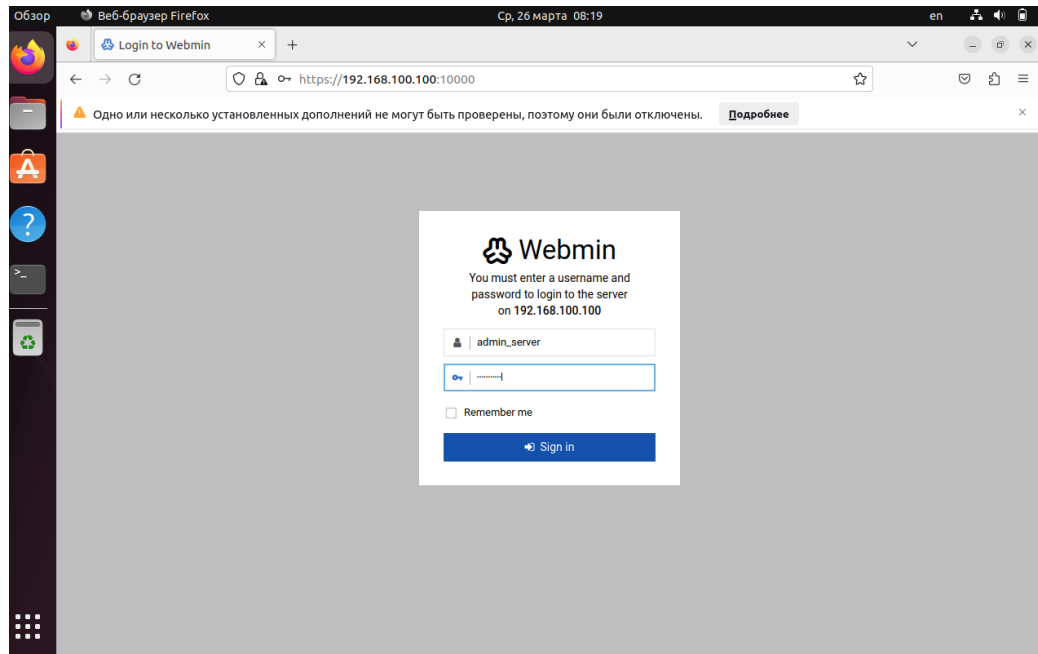
```
GNU nano 6.2 /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
/nfs/share_nfs 0.0.0.0/0(rw,sync,no_subtree_check)
```

```
admin_server@server-ubuntu2204:~$ sudo exportfs -a
```

```
admin_server@server-ubuntu2204:~$ sudo ufw allow 111
Rules updated
Rules updated (v6)
admin_server@server-ubuntu2204:~$ sudo ufw allow 2049
Rules updated
Rules updated (v6)
admin_server@server-ubuntu2204:~$ _
```

8. Настроить сервер NFS с помощью программы Webmin

8.1. Необходимо настроить общий доступ к каталогу / nfs / sharer_nfs для всех пользователей только для чтения.



← ?

☆ Создание каталога

Настройка каталога

Экспортируемый каталог

/nfs/sharer_nfs

Включить

☒ Да ☐ Нет

Доступен для..

☒ Всех

☐ Указанных узлов

☐ Сетевой группы

☐ Сеть IPv4

☐ Сеть IPv6

Маска сети

Защита каталога

Только для чтения

☒ Да ☐ Нет

Клиенты должны быть на защищенном порту

☒ Да ☐ Нет

Отключить проверку поддерева

☐ Да ☒ Нет

Скрыть файловую систему

☐ Да ☒ Нет

Сразу синхронизировать все пишете

☐ да ☐ нет ☒ По умолчанию

Доверять удаленным пользователям

Считать ненадежных пользователей

☒ По умолчанию

Считать ненадежные группы

☒ По умолчанию

Делать символьные ссылки относительными

☐ Да ☒ Нет

Запретить доступа к каталогу

☐ Да ☒ Нет

⚙ ?

☆ Экспортируемые каталоги NFS

☰

☒ Выбрать все ☒ Инвертировать выбор ☐ Добавить каталог для экспорта ☐ Добавьте новый экспорт NFSv4

Каталог	Доступен для..
<input type="checkbox"/> /srv/homes	Узлы hostname1 (Отключен) Узлы hostname2 (Отключен)
<input type="checkbox"/> /srv/nfs4	Сеть с проверкой подлинности: gss/krb5i (Отключен)
<input type="checkbox"/> /srv/nfs4/homes	Сеть с проверкой подлинности: gss/krb5i (Отключен)
<input type="checkbox"/> /nfs/share_nfs	Сети 0.0.0.0/0
<input type="checkbox"/> /nfs/sharer_nfs	Всем

☒ Выбрать все ☒ Инвертировать выбор ☐ Добавить каталог для экспорта ☐ Добавьте новый экспорт NFSv4

✖ Удалить выбранные экспорты

☐ Отключить выбранное

☒ Включить выбранное

☒ Применить изменения

Нажатие на эту кнопку приведет к применению текущей конфигурации экспортируемых каталогов. Все перечисленные выше каталоги станут доступны в соответствии с указанными для них настройками.

☆ Обновить модули

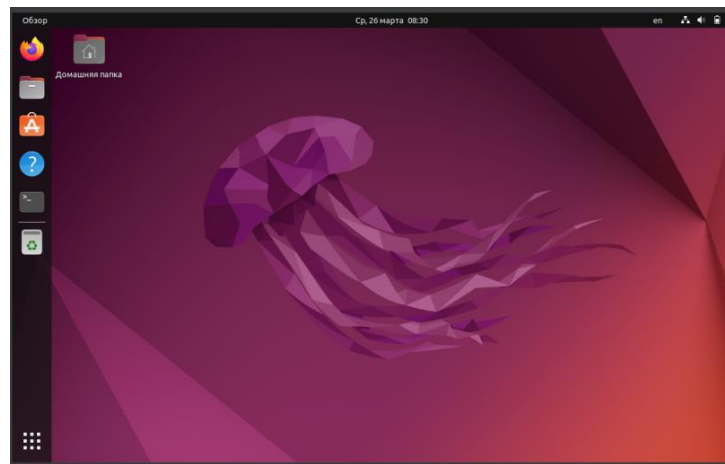
Проверка используемых модулей Webmin ..

.. обнаружены 58 с установленными приложениями, и 46 с неустановленными.


```
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
nfs/share_nfs 0.0.0.0/0(rw,sync,no_subtree_check)
nfs/sharer_nfs (no_root_squash,nohide,ro)
```

9. Установить клиента файловой системы NFS

9.1. перейти на виртуальную машину ws1-ubuntu2204



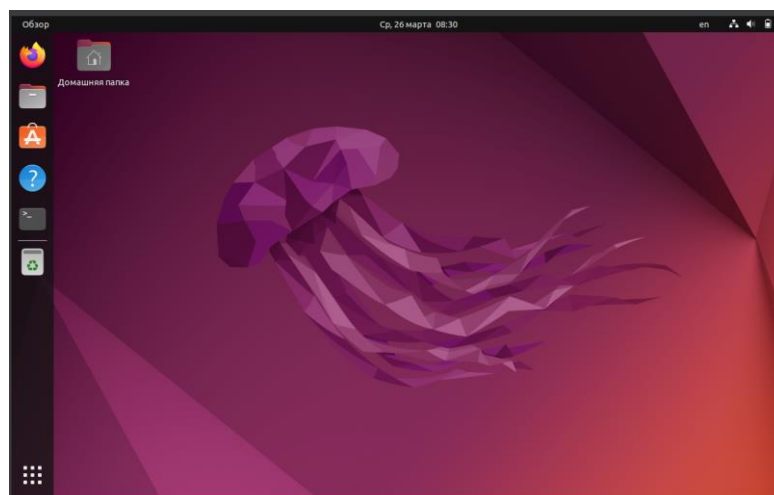
9.2. выполнить команды установки пакета клиента NFS

```
admin_ws@ws1-ubuntu2204:~$ sudo apt-get update
[sudo] пароль для admin_ws: 
```

```
admin_ws@ws1-ubuntu2204:~$ sudo apt-get install nfs-common
```

10. Настроить клиента NFS для доступа к сетевому каталогу с использованием статического монтирования

10.1. перейти на рабочую станцию ws1-ubuntu2204



10.2. создать точки монтирования для каталогов NFS

/mnt/client_nfs/

/mnt/clientr_nfs/

```
admin_ws@ws1-ubuntu2204:~$ sudo mkdir -p /mnt/client_nfs/  
admin_ws@ws1-ubuntu2204:~$ sudo mkdir -p /mnt/clientr_nfs/
```

10.3. монтировать каталоги сервера NFS в точки монтирования клиента:

10.3.1. каталог сервера /nfs/share_nfs в точку монтирования /mnt/client_nfs /

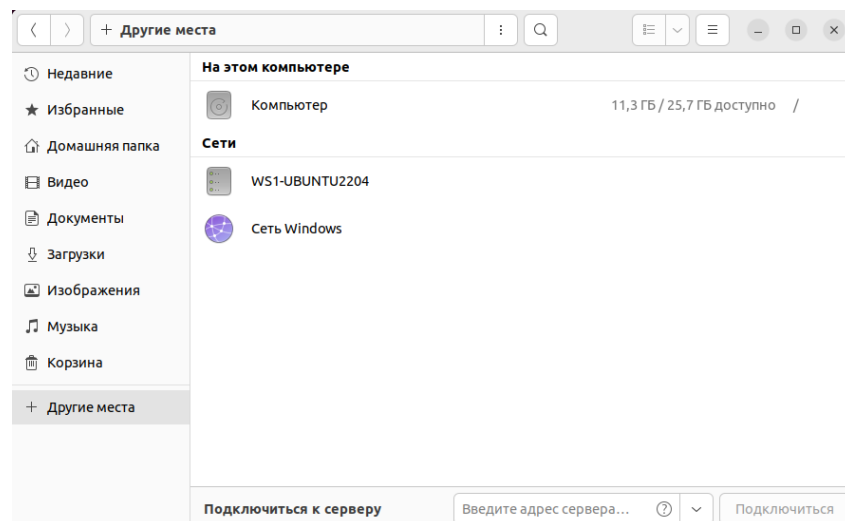
```
admin_ws@ws1-ubuntu2204:~$ sudo mount 192.168.100.100:/nfs/share_nfs /mnt/client_nfs
```

10.3.2. каталог сервера /nfs/sharer_nfs в точку монтирования /mnt/clientr_nfs /

```
admin_ws@ws1-ubuntu2204:~$ sudo mount -v -o rw 192.168.100.100:/nfs/sharer_nfs /mnt/clientr_nfs  
mount.nfs: timeout set for Wed Mar 26 10:01:01 2025  
mount.nfs: trying text-based options 'vers=4.2,addr=192.168.100.100,clientaddr=192.168.100.101'
```

10.4. в графической оболочке открыть каталог admin_ws

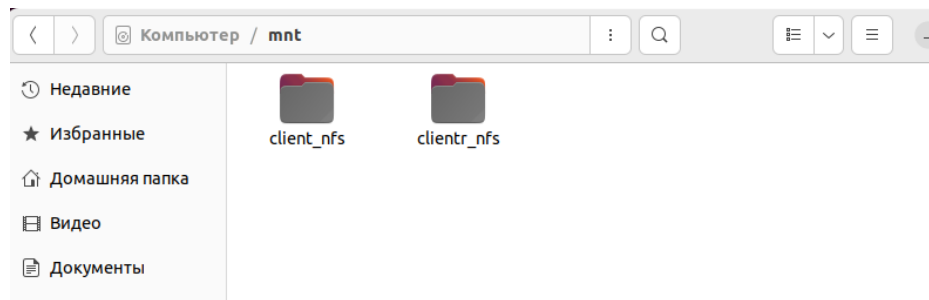
10.5. выбрать + Другие места



10.6. выбрать Компьютер

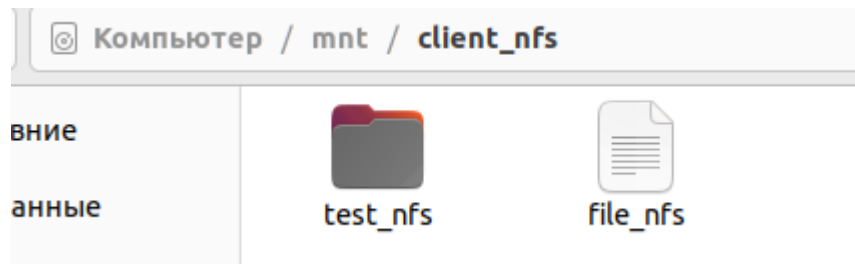
10.7. открыть каталог mnt

10.8. открыть каталоги share_nfs и sharer_nfs



10.9. просмотреть свойства каталога

10.10. создать в каталог вложенные каталоги и файлы



```
admin_server@server-ubuntu2204:~$ ls -la /nfs/share_nfs
total 12
drwxrwxrwx 3 admin_nfs admin_nfs 4096 map 26 07:03
drwxrwxrwx 4 admin_nfs admin_nfs 4096 map 26 05:00
-rwxrwxrwx 1 admin_nfs admin_nfs 0 map 26 05:02 file_nfs
drwxrwxr-x 2 admin_server admin_server 4096 map 26 07:03 test_nfs
admin_server@server-ubuntu2204:~$ _
```

10.11. размонтировать каталог

```
admin_ws@ws1-ubuntu2204:~$ sudo umount /mnt/client_nfs
admin_ws@ws1-ubuntu2204:~$ sudo umount /mnt/clientr_nfs
```

11. Настроить доступ к сетевому каталогу NFS с использованием автомонтирования

11.1. Выполнить настройку автомонтирования сетевого каталога NFS при обращении к нему и установить значение тайм-аута для удержания данного соединения.

```
admin_ws@ws1-ubuntu2204:~$ sudo apt install autofs
```

```
admin_ws@ws1-ubuntu2204:~$ sudo nano /etc/auto.master
```

```
GNU nano 6.2 /etc/aut
#
+dir:/etc/auto.master.d
#
# If you have fedfs set up and the related binaries, either
# built as part of autofs or installed from another package,
# uncomment this line to use the fedfs program map to access
# your fedfs mounts.
#/nfs4 /usr/sbin/fedfs-map-nfs4 nobind
#
# Include central master map if it can be found using
# nsswitch sources.
#
# Note that if there are entries for /net or /misc (as
# above) in the included master map any keys that are the
# same will not be seen as the first read key seen takes
# precedence.
#
+auto.master
/mnt /etc/auto.nfs --timeout=300

admin_ws@ws1-ubuntu2204:~$ sudo nano /etc/auto.nfs
```

```
admin_ws@ws1-ubuntu2204: ~
GNU nano 6.2 /etc
share_nfs -fstype=nfs4,rw 192.168.100.100:/nfs/share_nfs
sharer_nfs -fdtype=nfs4,rw 192.168.100.100:/nfs/sharer_nfs

admin_ws@ws1-ubuntu2204:~$ sudo systemctl restart autofs

admin_ws@ws1-ubuntu2204:~$ ls -la /mnt/share_nfs
итого 8
drwxrwxrwx 3      1004      1006 4096 map 26 10:03 .
drwxr-xr-x 3 root      root      0 map 26 10:15 ..
-rwxrwxrwx 1      1004      1006  0 map 26 08:02 file_nfs
drwxrwxr-x 2 admin_ws admin_ws 4096 map 26 10:03 test_nfs
```

Контрольные вопросы

1. Назовите особенности файловой системы NFS.

NFS (Network File System) имеет следующие особенности:

- Сетевая файловая система: Основная особенность - предоставляет возможность совместного доступа к файлам и каталогам по сети. Клиенты NFS могут обращаться к файлам, расположенным на сервере, так, как если бы они находились на локальном диске.

- Независимость от платформы: NFS разработана таким образом, чтобы быть платформенно-независимой. Это позволяет клиентам и серверам под управлением различных операционных систем (например, Linux, Unix, macOS) взаимодействовать друг с другом.
- Прозрачность: Для пользователей доступ к файлам, хранящимся на NFS-сервере, часто выглядит так же, как и доступ к локальным файлам. Приложения могут работать с этими файлами, не зная о том, что они хранятся удаленно.
- Различные версии: Существует несколько версий NFS (v2, v3, v4). Версия 4 включает в себя улучшения в плане безопасности, производительности и поддержки межсетевого взаимодействия.
- Бесплатная (как правило): В большинстве дистрибутивов Linux и Unix, NFS входит в стандартный набор утилит и является бесплатной для использования.
- Состояние без сохранения состояния (Stateless - до NFSv4): В более старых версиях (до v4) NFS сервер не сохранял информацию о состоянии клиентских подключений. Это упрощало его реализацию, но делало менее надежным в случае сбоев. NFSv4 ввела концепцию состояния, что повысило надежность.
- Централизованное управление: NFS позволяет централизованно хранить данные и управлять доступом к ним, что упрощает администрирование и обслуживание.
- Иерархическая структура: Поддерживает стандартную иерархическую структуру каталогов.

2. Для чего предназначен файловый сервер NFS?

Файловый сервер NFS предназначен для:

- Предоставления доступа к файлам и каталогам по сети: Это основная функция. Сервер позволяет нескольким клиентам одновременно получать доступ к файлам, хранящимся на сервере.

- **Централизованного хранения данных:** Вместо того, чтобы хранить файлы на каждой рабочей станции, их можно хранить на сервере NFS, что упрощает резервное копирование, управление версиями и администрирование.
- **Совместного использования файлов:** Пользователи могут совместно работать с документами, проектами и другими файлами, хранящимися на сервере NFS.
- **Упрощения администрирования:** Централизованное хранение данных упрощает задачи администрирования, такие как обновление программного обеспечения, установка патчей безопасности и резервное копирование.
- **Экономии дискового пространства:** Можно избежать дублирования файлов на нескольких компьютерах, используя общий доступ к файлам на сервере NFS.
- **Развертывания сетевых приложений:** NFS может использоваться для хранения данных, используемых сетевыми приложениями, такими как базы данных, веб-серверы и почтовые серверы.

3. Какие ресурсы могут быть общими в NFS?

В NFS общими могут быть:

1. **Каталоги:** Это наиболее распространенный тип ресурса, предоставляемого в NFS. Сервер может предоставить доступ к одному или нескольким каталогам, включая все подкаталоги и файлы в них.
2. **Файлы (реже):** Хотя менее распространено, можно предоставить доступ к отдельным файлам.
3. **Файловые системы (точки монтирования):** В принципе, можно экспортировать всю файловую систему, но это обычно не рекомендуется из соображений безопасности и управления. Чаще экспортируют конкретные каталоги, расположенные внутри файловой системы.

Важно отметить, что нельзя напрямую экспортировать отдельные разделы диска. NFS работает на уровне файловой системы. Сначала нужно создать файловую систему на разделе, а затем экспортировать каталог внутри этой файловой системы.

4. В чём заключается различие статического монтирования и автомонтирования?

- Статическое монтирование:
 - Определяется в файле `/etc/fstab`.
 - Монтирование происходит автоматически при загрузке системы или при выполнении команды `mount -a`.
 - Соединение с NFS-сервером устанавливается и поддерживается постоянно, даже если ресурсы не используются.
 - Подходит для ресурсов, которые используются часто и регулярно.
 - Проще в настройке.
- Автомонтирование:
 - Использует демон `automount` (или аналогичный), который автоматически монтирует и размонтирует файловые системы по мере необходимости.
 - Монтирование происходит только при обращении к точке монтирования (например, при попытке открыть файл в каталоге, который должен быть примонтирован).
 - Файловая система автоматически размонтируется после периода бездействия, освобождая ресурсы.
 - Подходит для ресурсов, которые используются нечасто, экономя ресурсы (сетевой трафик, соединения).
 - Более сложная настройка, требующая конфигурирования `automount`.

- Увеличивает нагрузку на систему, так как требует постоянного мониторинга точек монтирования.



**Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)**

ФАКУЛЬТЕТ Информатика и системы управления

КАФЕДРА Системы обработки информации и управления

Отчет по лабораторной работе № 5

**«Сетевые интерфейсы рабочих станций и серверов ОС Alt Linux.
Средства удалённого администрирования»
по дисциплине «Сетевое программное обеспечение»**

Студент ИУ5-61Б
(Группа)

Е.И. Бирюкова
(Подпись, дата) (И.О.Фамилия)

Преподаватель

П.С. Семкин
(Подпись, дата) (И.О.Фамилия)

Москва

2025

Цель работы

Целью работы является приобретение навыков:

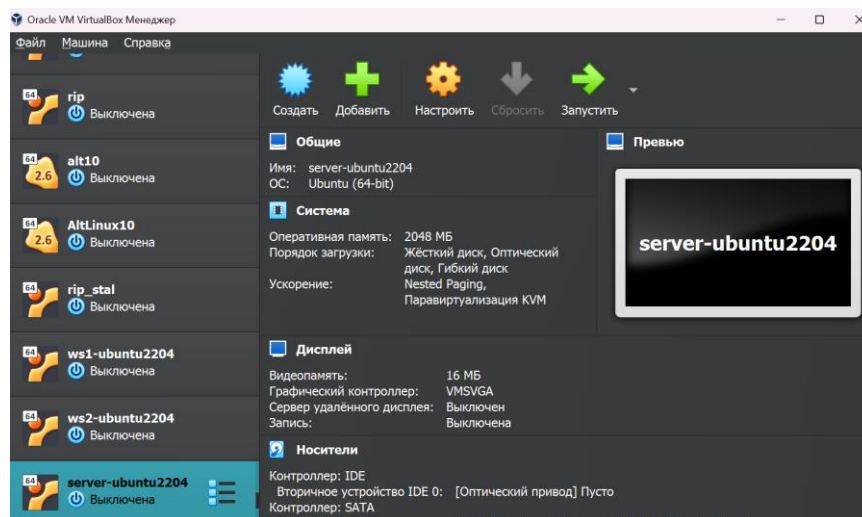
1. настройки сетевых интерфейсов рабочих станции и серверов Alt Linux,
2. создания локальной IP-сети,
3. использования средств удаленного администрирования.

Задание

1. Установить виртуальные машины рабочих станций с операционными системами Alt-Рабочая станция и Alt-сервер.
2. Подключить сетевые адаптеры виртуальных машин для подключения к внешней сети и локальной сети.
3. Запустить виртуальные машины
4. Установить пакет Netplan на рабочую станцию и сервер
5. С помощью текстового редактора описать на языке YAML сетевые конфигурации рабочей станции и сервера. Для рабочей станции использовать сетевой менеджер NetworkManager, а для сервера – сетевой менеджер systemd-networkd
6. Командами Netplan создать конфигурационные файлы сетевых менеджеров рабочей станции и сервера
7. Проверить правильность установки IP-адресов рабочих станций локальной сети
8. Настроить средства удалённого администрирования – протокол SSH и Центр Управления Системой

Порядок выполнения работы

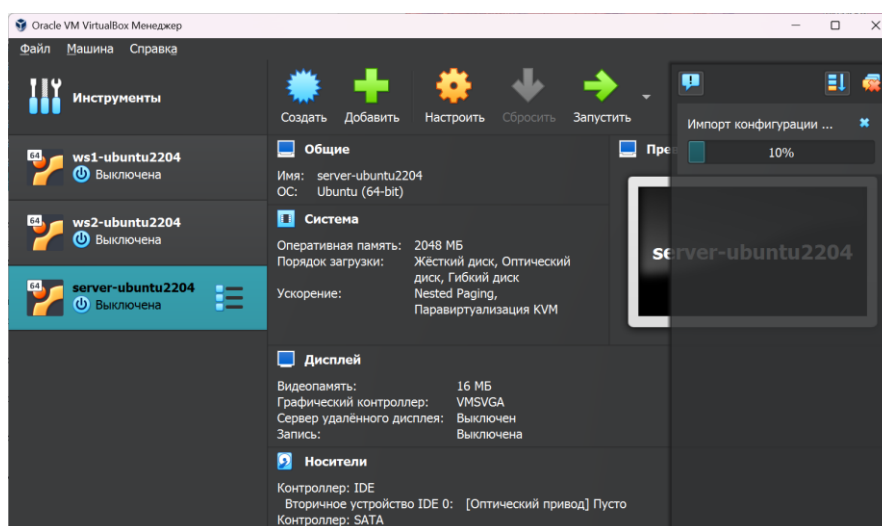
1. Войти в систему под учётной записью stud_XX, где XX - индекс группы.
Пароль studXX
2. Запустить программу виртуализации Oracle VM VirtualBox



3. Установить и настроить виртуальную машину ws1-alt10

3.1.Импортировать виртуальную машину ws1-Alt10 с установленной операционной системой Alt Рабочая станция:

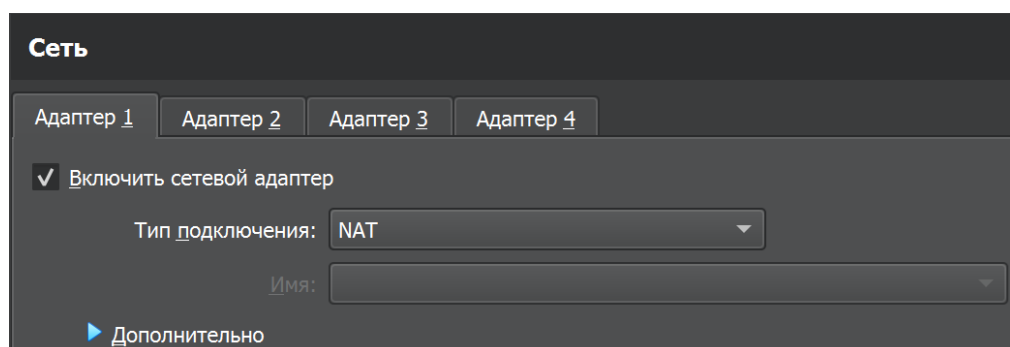
\\home\ОС-СПО\Сети Alt \ ws1-alt10.ova



3.2.В настройках Сеть машины

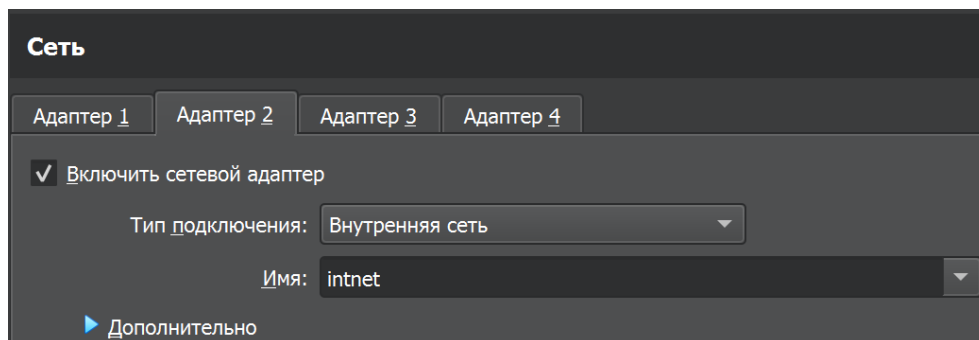
3.2.1. включить Адаптер 1

3.2.2. выбрать тип подключения: NAT

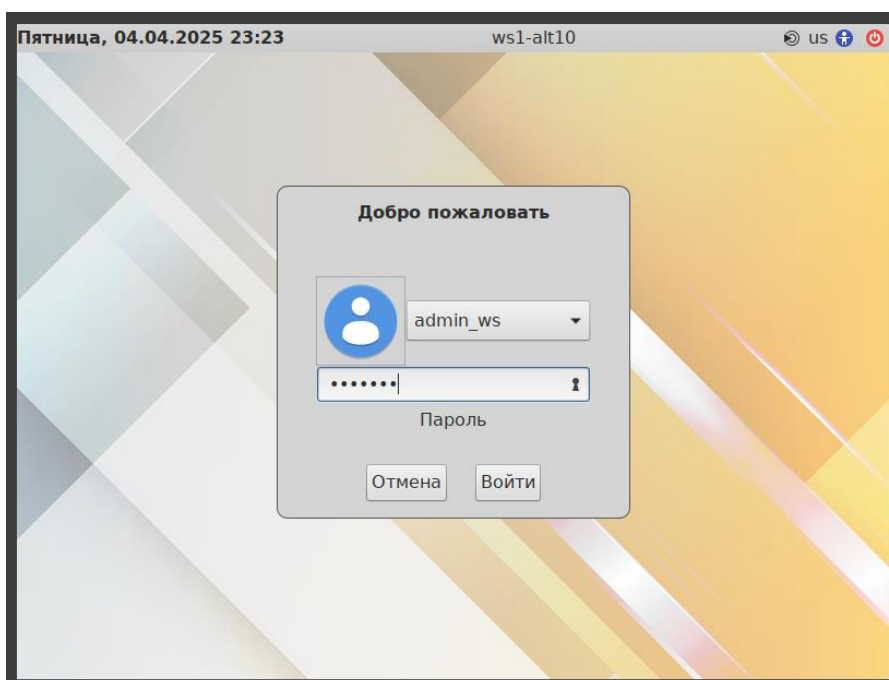


3.2.3. включить Адаптер 2

3.2.4. выбрать тип подключения: Внутренняя сеть



3.3. Запустить рабочую станцию ws1-alt10 (пользователь admin_ws пароль adminws)



4. Настроить сетевые интерфейсы рабочей станции ws1-alt10

4.1. Необходимо на ws1-alt10 настроить сетевые интерфейсы для выхода в Интернет через хост-компьютер и для связи с узлами локальной сети.

4.2. Для этого необходимо настроить два сетевых интерфейса – enp0s3 для выхода во внешнюю сеть, и enp0s8 для связи с локальной сетью.

Интерфейсу enp0s3 будет назначаться IP-адрес от внешнего DHCP-сервера программы виртуализации VirtualBox. Если в процессе установки рабочей станции хост-компьютер был подключен к Интернету, то интерфейс enp0s3 активируется автоматически.

4.3.Интерфейс enp0s8 предназначен для назначение рабочей станции статического IP-адреса 192.168.100.101 и маски 255.255.255.0 для работы в локальной сети.

4.4.Войти в систему под учётной записью root

```
ws1-alt10 login: root
Password:
Last login: Fri Apr  4 23:47:13 MSK 2025 on tty2
ws1-alt10 ~ # _
```

4.5.Установить на рабочей станции пакет netplan

```
ws1-alt10 ~ # apt-get update
Get:1 http://mirror.yandex.ru p10/branch/x86_64 release [4215B]
Get:2 http://mirror.yandex.ru p10/branch/x86_64-i586 release [1665B]
Get:3 http://mirror.yandex.ru p10/branch/noarch release [2836B]
Fetched 8716B in 0s (137kB/s)
Get:1 http://mirror.yandex.ru p10/branch/x86_64/classic pkglist [24.5MB]
28% [1 pkglist 6968308/24.5MB 28%]_
```

root: apt-get upgrade

```
ws1-alt10 ~ # apt-get install netplan
Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
  python3-module-Pygments python3-module-markdown-it python3-module-mdurl python3-module-netifaces
  python3-module-rich python3-module-yaml
The following NEW packages will be installed:
  netplan python3-module-Pygments python3-module-markdown-it python3-module-mdurl
  python3-module-netifaces python3-module-rich python3-module-yaml
0 upgraded, 7 newly installed, 0 removed and 0 not upgraded.
Need to get 2932kB of archives.
After unpacking 15.1MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

```
ws1-alt10 ~ # apt-get install nano
Reading Package Lists... Done
Building Dependency Tree... Done
nano is already the newest version.
0 upgraded, 0 newly installed, 0 removed and 0 not upgraded.
```

4.6.Описать сетевую конфигурацию рабочей станции на языке разметки

YAML в файле /etc/netplan/config.yaml

```
ws1-alt10 ~ # nano /etc/netplan/config.yaml
```

```
GNU nano 7.2 /etc/netplan/config.yaml
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: true
      dhcp6: no
  ethernets:
    enp0s8:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.100.101/24]_
```

4.7. Создать файл конфигурации для выбранного сетевого менеджера

```
ws1-alt10 ~ # netplan apply

** (generate:25572): WARNING **: 15:37:44.192: Permissions for /etc/netplan/config.yaml are too open.
. Netplan configuration should NOT be accessible by others.

** (process:25570): WARNING **: 15:37:44.835: Permissions for /etc/netplan/config.yaml are too open.
. Netplan configuration should NOT be accessible by others.

** (process:25570): WARNING **: 15:37:45.491: Permissions for /etc/netplan/config.yaml are too open.
. Netplan configuration should NOT be accessible by others.

** (process:25570): WARNING **: 15:37:45.492: Permissions for /etc/netplan/config.yaml are too open.
. Netplan configuration should NOT be accessible by others.
ws1-alt10 ~ # netplan generate

** (generate:26063): WARNING **: 15:37:58.173: Permissions for /etc/netplan/config.yaml are too open.
. Netplan configuration should NOT be accessible by others.
```

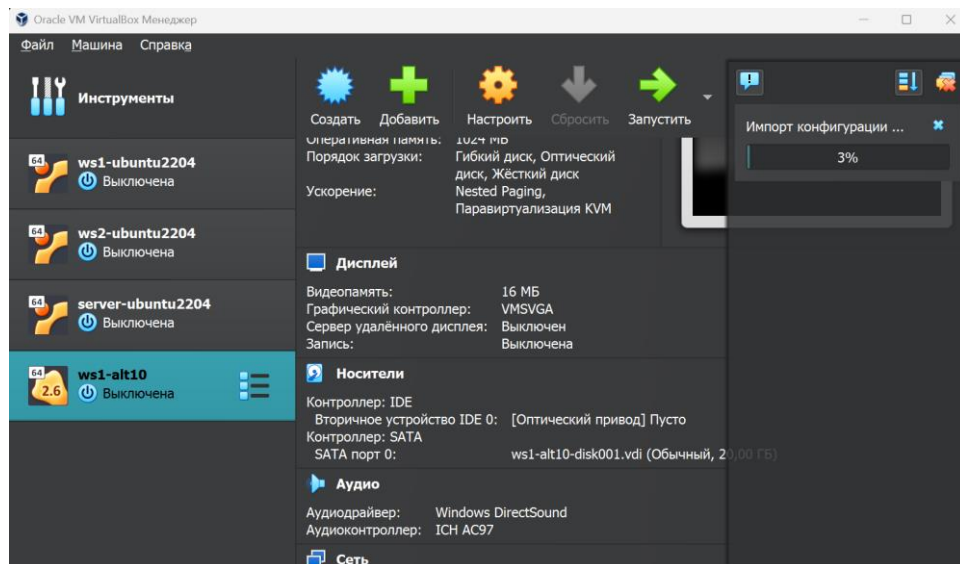
4.8. Просмотреть сетевые интерфейсы рабочей станции

```
ws1-alt10 ~ # ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:dd:d8:4b brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86290sec preferred_lft 86290sec
    inet6 fe80::a00:27ff:fedd:d84b/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e4:cf:63 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.101/24 brd 192.168.100.255 scope global noprefixroute enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee4:cf63/64 scope link
        valid_lft forever preferred_lft forever
```

5. Установить и настроить виртуальную машину server-alt10

5.1. Импортировать виртуальную машину server-Alt10 с установленной операционной системой Alt сервер:

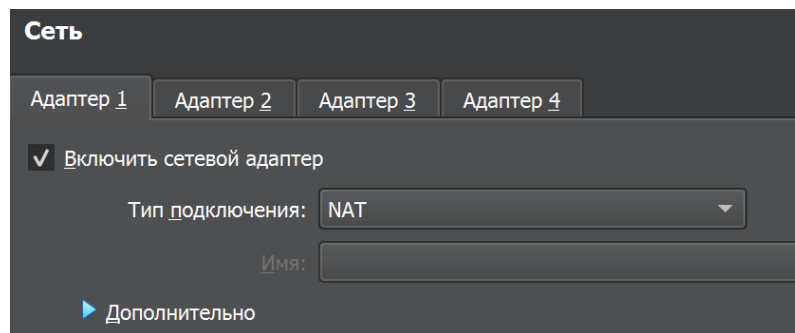
\\home\\ОС-СПО\\Сети Alt \\ server-alt10.ova



5.2. В настройках Сеть виртуальной машины

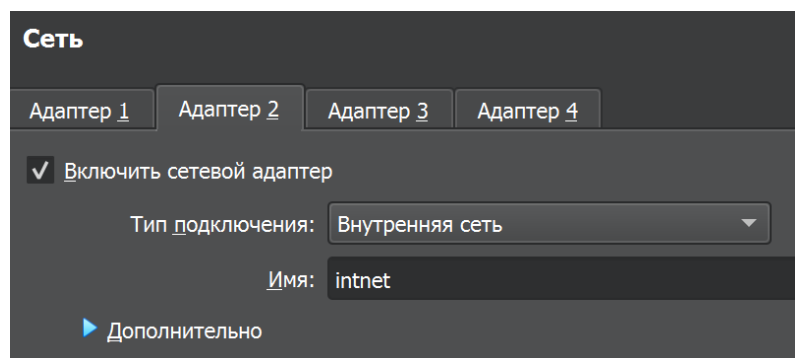
5.2.1. включить Адаптер 1

5.2.2. выбрать тип подключения: NAT



5.2.3. включить Адаптер 2

5.2.4. выбрать тип подключения: Внутренняя сеть



5.3. Запустить сервер server-alt10 (пользователь root пароль adminroot)

```
server-alt10 login: root
Password:
Last login: Sat Jan 7 19:39:58 MSK 2023 on tty1
[root@server-alt10 ~]# _
```

6. Настроить сетевые интерфейсы сервера server-alt10

6.1. Необходимо на server-alt10 настроить сетевые интерфейсы для выхода в Интернет через хост-компьютер и для связи с узлами локальной сети.

6.2. Для этого необходимо настроить два сетевых интерфейса – enp0s3 для выхода во внешнюю сеть, и enp0s8 для связи с локальной сетью.

6.3. Интерфейсу enp0s3 будет назначаться IP-адрес от внешнего DHCP-сервера программы виртуализации VirtualBox. Если в процессе установки рабочей станции хост-компьютер был подключен к Интернету, то интерфейс enp0s3 активируется автоматически.

6.4. Интерфейс enp0s8 предназначен для назначения рабочей станции статического IP-адреса 192.168.100.100 и маски 255.255.255.0 для работы в локальной сети.

6.5. Установить на сервере пакеты netplan и nano

```
[root@server-alt10 ~]# apt-get update
Get:1 http://mirror.yandex.ru p10/branch/x86_64 release [4215B]
Get:2 http://mirror.yandex.ru p10/branch/x86_64-i586 release [1665B]
Get:3 http://mirror.yandex.ru p10/branch/noarch release [2836B]
Fetched 8716B in 0s (65.4kB/s)
Get:1 http://mirror.yandex.ru p10/branch/x86_64/classic pkglist [24.5MB]
24% [1 pkglist 6019157/24.5MB 24%]
```

```
[root@server-alt10 ~]# apt-get install netplan
Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
```

```
[root@server-alt10 ~]# apt-get install nano
Reading Package Lists... Done
Building Dependency Tree... Done
```

6.6. Описать сетевую конфигурацию сервера на языке разметки YAML в файле /etc/netplan/config.yaml

```
[root@server-alt10 ~]# nano /etc/netplan/config.yaml
```

```
GNU nano 7.2 /etc/netplan/config.yaml
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: true
      dhcp6: no
    ethernets:
      enp0s8:
        dhcp4: no
        dhcp6: no
        addresses: [192.168.100.100/24]
```

6.7. Создать файл конфигурации для выбранного сетевого менеджера


```
[root@server-alt10 ~]# netplan apply

** (generate:3449): WARNING **: 15:54:30.058: Permissions for /etc/netplan/config.yaml are too open. Netplan configuration should NOT be accessible by others.
Cannot call openuswitch: ovsdb-server.service is not running.

** (process:3447): WARNING **: 15:54:30.292: Permissions for /etc/netplan/config.yaml are too open. Netplan configuration should NOT be accessible by others.

** (process:3447): WARNING **: 15:54:30.373: Permissions for /etc/netplan/config.yaml are too open. Netplan configuration should NOT be accessible by others.

** (process:3447): WARNING **: 15:54:30.378: Permissions for /etc/netplan/config.yaml are too open. Netplan configuration should NOT be accessible by others.
[root@server-alt10 ~]# netplan generate

** (generate:3652): WARNING **: 15:54:52.648: Permissions for /etc/netplan/config.yaml are too open. Netplan configuration should NOT be accessible by others.
```

6.8. Просмотреть сетевые интерфейсы сервера

```
[root@server-alt10 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4d:40:0c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86351sec preferred_lft 75551sec
    inet6 fe80::a00:27ff:fe4d:400c/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:24:3d:ad brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.100/24 brd 192.168.100.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe24:3dad/64 scope link
        valid_lft forever preferred_lft forever
```

7. Проверить сетевые соединения сервера и рабочей станции IP-сети

7.1. Проверить сетевое соединение клиента и сервера сети.

```
[admin_ws@ws1-alt10 ~]$ ping 192.168.100.100
PING 192.168.100.100 (192.168.100.100) 56(84) bytes of data.
64 bytes from 192.168.100.100: icmp_seq=1 ttl=64 time=2.05 ms
64 bytes from 192.168.100.100: icmp_seq=2 ttl=64 time=1.07 ms
64 bytes from 192.168.100.100: icmp_seq=3 ttl=64 time=0.889 ms
64 bytes from 192.168.100.100: icmp_seq=4 ttl=64 time=1.54 ms
64 bytes from 192.168.100.100: icmp_seq=5 ttl=64 time=1.06 ms
^C
--- 192.168.100.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.889/1.320/2.046/0.423 ms
```

```
[root@server-alt10 ~]# ping 192.168.100.101
PING 192.168.100.101 (192.168.100.101) 56(84) bytes of data.
64 bytes from 192.168.100.101: icmp_seq=1 ttl=64 time=0.765 ms
64 bytes from 192.168.100.101: icmp_seq=2 ttl=64 time=1.11 ms
64 bytes from 192.168.100.101: icmp_seq=3 ttl=64 time=1.11 ms
64 bytes from 192.168.100.101: icmp_seq=4 ttl=64 time=1.04 ms
64 bytes from 192.168.100.101: icmp_seq=5 ttl=64 time=1.07 ms
^C
--- 192.168.100.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.765/1.018/1.112/0.129 ms
```

8. Настроить службу SSH для удалённого доступа к серверу

8.1. Создать на сервере server-alt10 пользователя admin_ssh

```
[root@server-alt10 ~]# useradd admin_ssh
[root@server-alt10 ~]# passwd admin_ssh
```

8.2. Проверить статус службы SSH на сервере и рабочей станции

```
[root@server-alt10 ~]# systemctl status sshd
sshd.service - OpenSSH server daemon
  Loaded: loaded (/lib/systemd/system/sshd.service; enabled; vendor preset:
  Active: active (running) since Sat 2025-04-05 15:43:08 MSK; 21min ago
  Main PID: 2496 (sshd)
  Tasks: 1 (limit: 1159)
  Memory: 2.0M
  CPU: 20ms
  CGroup: /system.slice/sshd.service
          └─2496 /usr/sbin/sshd -D

Apr 05 15:43:07 server-alt10 systemd[1]: Starting OpenSSH server daemon...
Apr 05 15:43:08 server-alt10 systemd[1]: Started OpenSSH server daemon.
Apr 05 15:43:08 server-alt10 sshd[2496]: Server listening on 0.0.0.0 port 22.
Apr 05 15:43:08 server-alt10 sshd[2496]: Server listening on :: port 22.
```

8.3. При необходимости включить службы

8.4. Изменить порт, на котором должна работать служба.

На сервере

```
[root@server-alt10 ~]# systemctl stop sshd
[root@server-alt10 ~]# nano /etc/openssh/sshd_config
```

```
GNU nano 7.2 /etc/openssh/sshd_config
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/bin:/usr/bin:/usr/local/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Port 2222
#AddressFamily any
```

```
[root@server-alt10 ~]# systemctl start sshd
```

```
[root@server-alt10 ~]# systemctl status sshd
sshd.service - OpenSSH server daemon
  Loaded: loaded (/lib/systemd/system/sshd.service; enabled; vendor preset:
  Active: active (running) since Sat 2025-04-05 16:08:05 MSK; 2min 13s ago
  Process: 3690 ExecStartPre=/usr/bin/ssh-keygen -A (code=exited, status=0/SU
  Process: 3691 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 3692 (sshd)
  Tasks: 1 (limit: 1159)
  Memory: 732.0K
  CPU: 13ms
  CGroup: /system.slice/sshd.service
          └─3692 /usr/sbin/sshd -D
```

```
[root@server-alt10 ~]# ss -tulnp | grep ssh
tcp  LISTEN 0      128          0.0.0.0:2222      0.0.0.0:*        users:((("ssd
",pid=3692,fd=3))
tcp  LISTEN 0      128          :::2222          :::*              users:((("ssd
",pid=3692,fd=4))
```

На рабочей станции

```
[root@ws1-alt10 ~]# nano /etc/openssh/sshd_config
```

```
root@ws1-alt10: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 7.2 /etc/openssh/sshd_config
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/bin:/usr/bin:/usr/local/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

```
[root@ws1-alt10 ~]# systemctl restart sshd
[root@ws1-alt10 ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/lib/systemd/system/sshd.service; disabled; vendor preset: enabled)
   Active: active (running) since Sat 2025-04-05 18:31:10 MSK; 6s ago
     Process: 3842 ExecStartPre=/usr/bin/ssh-keygen -A (code=exited, status=0/SUCCESS)
     Process: 3843 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 3844 (sshd)
       Tasks: 1 (limit: 1147)
      Memory: 752.0K
         CPU: 14ms
        CGroup: /system.slice/sshd.service
                └─ 3844 /usr/sbin/sshd -D

anp 05 18:31:10 ws1-alt10 systemd[1]: Stopping OpenSSH server daemon...
anp 05 18:31:10 ws1-alt10 systemd[1]: sshd.service: Deactivated successfully.
anp 05 18:31:10 ws1-alt10 systemd[1]: Stopped OpenSSH server daemon.
anp 05 18:31:10 ws1-alt10 systemd[1]: Starting OpenSSH server daemon...
anp 05 18:31:10 ws1-alt10 systemd[1]: Started OpenSSH server daemon.
anp 05 18:31:10 ws1-alt10 sshd[3844]: Server listening on 0.0.0.0 port 2222.
anp 05 18:31:10 ws1-alt10 sshd[3844]: Server listening on :: port 2222.
```

```
[root@ws1-alt10 ~]# ss -tulnp | grep ssh
tcp LISTEN 0      128          0.0.0.0:2222      0.0.0.0:*        users:((("sshd",
pid=3844,fd=3))
tcp LISTEN 0      128          [::]:2222        [::]:*          users:((("sshd",
pid=3844,fd=4))
```

8.5. Открыть на рабочей станции SSH-соединение с сервером

```
[admin_ws@ws1-alt10 ~]$ ssh admin_ssh@192.168.100.100
The authenticity of host '[192.168.100.100]:2222 ([192.168.100.100]:2222)' can't
be established.
ED25519 key fingerprint is SHA256:kD4h+VewXojqHbnCuR6WLkaCMv93bgs/4CSi6PYGU7M.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '[192.168.100.100]:2222' (ED25519) to the list of kno
wn hosts.
admin_ssh@192.168.100.100's password:
[admin_ssh@server-alt10 ~]$
```

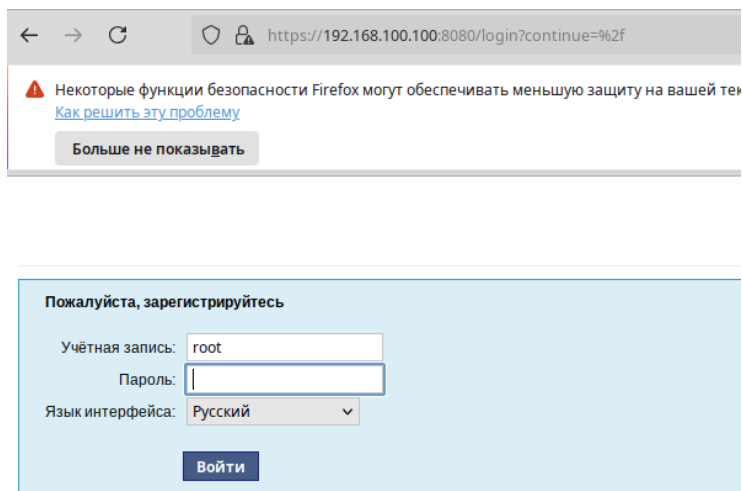
8.6. Закрывать SSH-соединение

```
[admin_ssh@server-alt10 ~]$ exit
Выход
Connection to 192.168.100.100 closed.
[admin_ws@ws1-alt10 ~]$
```

9. Настроить веб-интерфейс центра управления системой

9.1. На рабочей станции, используя веб-браузер Mozilla Firefox, подключиться к Центру Управления Системой сервера по ссылке <https://192.168.100.100:8080>

9.1.1. Учётная запись: root Пароль: adminroot



← → ↻ 🔒 <https://192.168.100.100:8080/login?continue=%2f>

⚠ Некоторые функции безопасности Firefox могут обеспечивать меньшую защиту на вашей те
[Как решить эту проблему](#)
Больше не показывать

Пожалуйста, зарегистрируйтесь

Учётная запись:

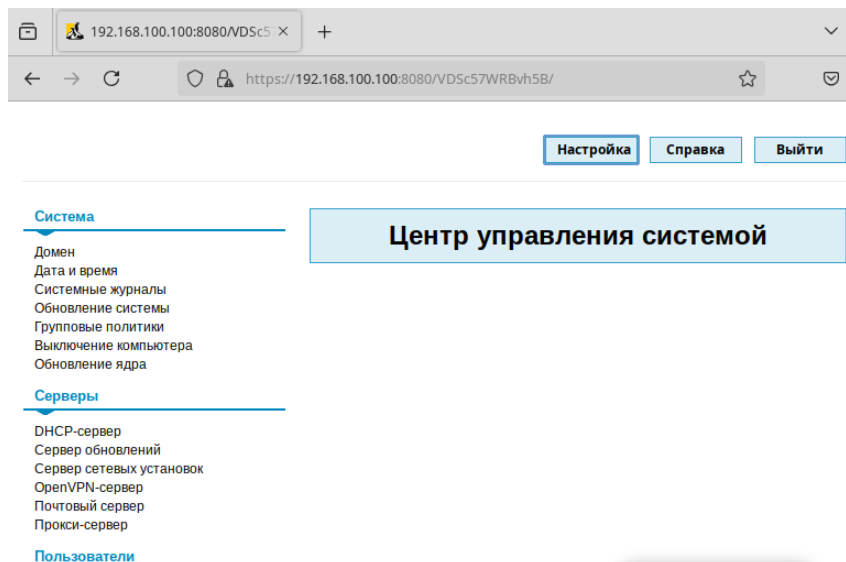
Пароль:

Язык интерфейса: Русский ▾

Войти

9.2. Ознакомиться с основными возможностями ЦУС

9.2.1. Установить параметры обновления системы



192.168.100.100:8080/VDSc5 X +

← → ↻ 🔒 <https://192.168.100.100:8080/VDSc57WRBvh5B/> ☆

Настройка Справка Выйти

Центр управления системой

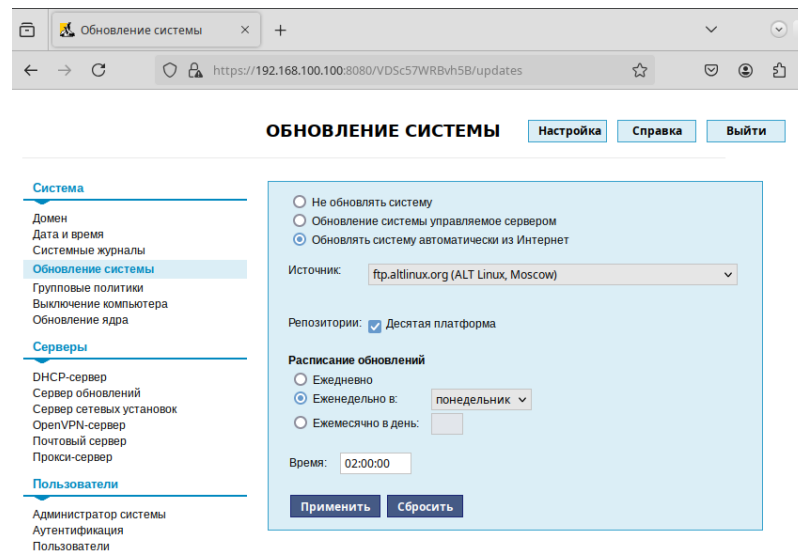
Система

- Домен
- Дата и время
- Системные журналы
- Обновление системы
- Групповые политики
- Выключение компьютера
- Обновление ядра

Серверы

- DNS-сервер
- Сервер обновлений
- Сервер сетевых установок
- OpenVPN-сервер
- Почтовый сервер
- Прокси-сервер

Пользователи



Контрольные вопросы

1. В чём заключается настройка сетевых интерфейсов рабочих станций сети?

Настройка сетевых интерфейсов рабочих станций сети включает в себя следующие шаги и аспекты:

- Определение сетевого интерфейса: Необходимо определить, какой сетевой интерфейс (например, eth0, enp0s3, wlan0) будет использоваться для подключения к сети. Это может быть проводной интерфейс Ethernet или беспроводной Wi-Fi.
- Назначение IP-адреса:
 - Статический IP-адрес: В этом случае IP-адрес, маска подсети, шлюз по умолчанию и DNS-серверы настраиваются вручную. Для этого используются инструменты командной строки (например, ip, ifconfig - хотя он устарел и лучше использовать ip) или графические утилиты (например, NetworkManager). В Alt Linux часто используют /etc/network/interfaces для конфигурации сети.
 - Динамический IP-адрес (DHCP): В этом случае рабочая станция получает IP-адрес, маску подсети, шлюз и DNS-серверы

автоматически от DHCP-сервера в сети. Для этого необходимо настроить сетевой интерфейс на получение адреса по DHCP.

- **Настройка DNS-серверов:** Необходимо указать IP-адреса DNS-серверов, которые будут использоваться для разрешения доменных имен в IP-адреса. Это может быть сделано вручную или автоматически, в зависимости от того, используется статический или динамический IP-адрес.
- **Настройка шлюза по умолчанию:** Необходимо указать IP-адрес шлюза по умолчанию, который будет использоваться для отправки трафика в другие сети (например, в Интернет). Это также может быть сделано вручную или автоматически.
- **Настройка маршрутизации (опционально):** В более сложных сетях может потребоваться настройка статических маршрутов для перенаправления трафика в определенные сети через определенные шлюзы.
- **Активация сетевого интерфейса:** После настройки необходимо активировать сетевой интерфейс, чтобы он начал работать. Это можно сделать с помощью команд `ip link set <интерфейс> up` или перезапуском сетевой службы (`systemctl restart networking`).
- **Тестирование соединения:** После настройки необходимо проверить, что рабочая станция может подключиться к сети и получить доступ к другим компьютерам и ресурсам в сети. Для этого можно использовать команды `ping`, `traceroute`, `nslookup` и другие сетевые утилиты.
- **Использование NetworkManager (обычно для графических сред):** В графических окружениях Alt Linux NetworkManager является распространенным инструментом для настройки сетевых соединений. Он предоставляет графический интерфейс для управления сетевыми интерфейсами, подключения к Wi-Fi сетям и настройки VPN.

- Файлы конфигурации: В Alt Linux (и других Linux-системах) информация о сетевых настройках обычно хранится в следующих файлах:
 - /etc/network/interfaces (если используется традиционный подход)
 - /etc/resolv.conf (для DNS-серверов, но часто управляется NetworkManager или DHCP-клиентом)
 - Файлы конфигурации NetworkManager (в каталоге /etc/NetworkManager/)

2. В каких случаях удобно использование статических IP-адресов рабочих станций?

Использование статических IP-адресов удобно в следующих случаях:

- Когда требуется постоянный и предсказуемый IP-адрес: Это важно для серверов, принтеров, сетевых устройств и других устройств, к которым должны обращаться другие компьютеры в сети. Например, если у вас есть веб-сервер или FTP-сервер, то ему нужен статический IP-адрес, чтобы пользователи могли всегда найти его по одному и тому же адресу.
- Когда требуется настройка статических маршрутов: Если в сети используются статические маршруты, то необходимо настроить статические IP-адреса для устройств, которые участвуют в маршрутизации.
- Когда требуется настройка правил брандмауэра: Если используются правила брандмауэра, которые основаны на IP-адресах, то необходимо настроить статические IP-адреса для устройств, к которым применяются эти правила.
- Для упрощения диагностики сети: Если все устройства в сети имеют статические IP-адреса, то легче отслеживать трафик и выявлять проблемы.

- Когда DHCP-сервер отсутствует или ненадежен: В небольших сетях, где нет DHCP-сервера или его работа нестабильна, использование статических IP-адресов может быть более надежным решением.
- Когда требуется доступ к рабочей станции извне сети: Если нужно обеспечить удаленный доступ к рабочей станции извне сети (например, через SSH или VNC), то статический IP-адрес значительно упрощает настройку перенаправления портов на маршрутизаторе.
- При использовании специфических приложений или сервисов: Некоторые приложения или сервисы могут требовать, чтобы устройства имели статические IP-адреса для корректной работы.



Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ Информатика и системы управления

КАФЕДРА Системы обработки информации и управления

Отчет по лабораторной работе № 6

**«Протокол передачи файлов FTP.
Установка и настройка FTP-сервера vsftpd и клиентов FTP»**
по дисциплине «Сетевое программное обеспечение»

Студент ИУ5-61Б
(Группа)

Е.И. Бирюкова
(Подпись, дата) (И.О.Фамилия)

Преподаватель

П.С. Семкин
(Подпись, дата) (И.О.Фамилия)

Москва

2025

Цель работы

Целью работы является приобретение навыков:

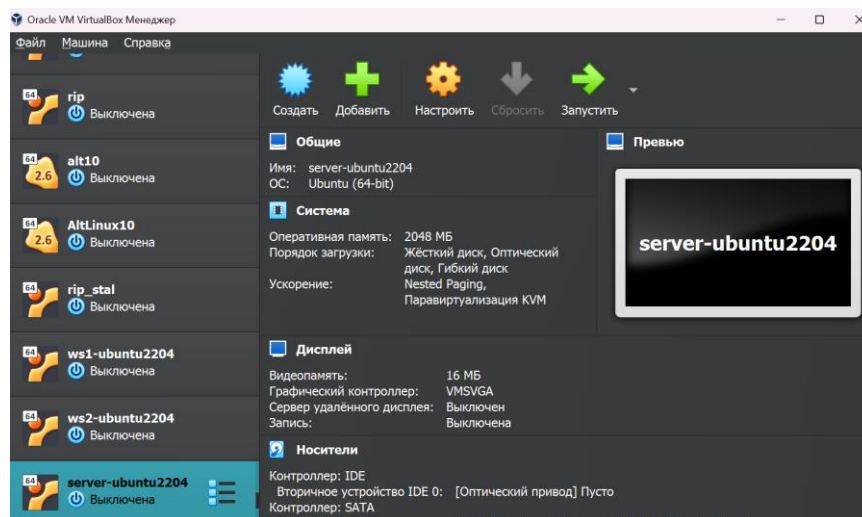
1. установки и запуска FTP-сервера vsftpd на сервер Alt Linux,
2. настройки FTP-сервера для анонимного доступа к серверу и доступа зарегистрированных пользователей
3. установки и настройки FTP-клиентов

Задание

1. Установить на сервер Alt Linux FTP-сервер vsftpd
2. Настроить FTP-сервер для анонимного доступа
3. Настроить FTP-сервер для доступа к серверу зарегистрированных пользователей
4. Создать на сервере каталоги и файлы для анонимного и авторизованного доступа
5. Настроить и запустить сервер vsftp через службу xinetd
6. Установить и настроить программу FTP-клиента ftp
7. Установить и настроить программу FTP-клиента FileZilla
8. Проверить работоспособность FTP-сервера

Порядок выполнения работы

1. Войти в систему под учётной записью stud_XX, где XX - индекс группы.
Пароль studXX
2. Запустить программу виртуализации Oracle VM VirtualBox

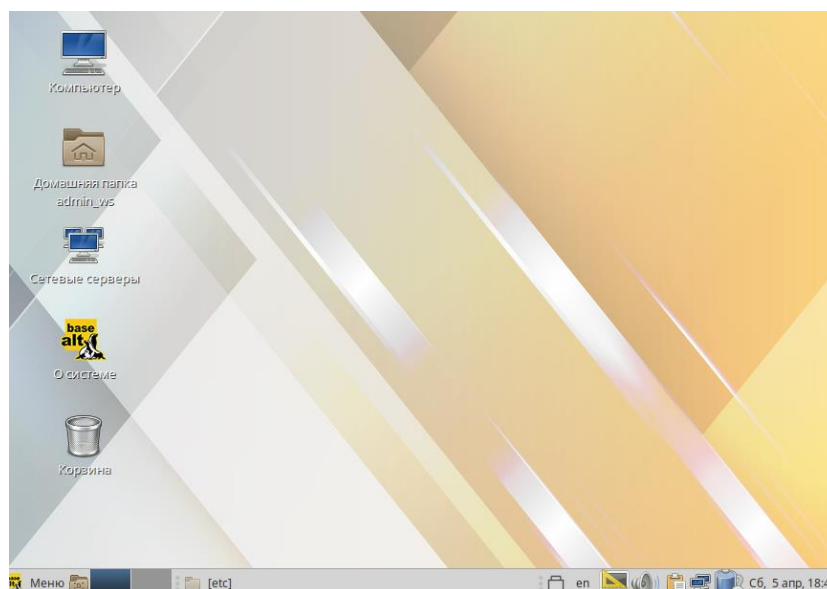


3. Запустить сервер и рабочую станцию локальной сети

3.1. Запустить виртуальную машину server-alt10 (пользователь admin_server пароль adminserver) с установленной операционной системой Alt сервер 10.0 и настроенными сетевыми интерфейсами.

```
[root@server-alt10 ~]#
```

3.2. Запустить рабочую станцию ws1-alt10 (пользователь admin_ws пароль adminws) с установленной операционной системой Alt Рабочая станция 10.0 и настроенными сетевыми интерфейсами.



4. Создать пользователей и каталоги на сервере server-alt10

4.1. Перейти на сервер server-alt10

```
[root@server-alt10 ~]#
```

4.2. Установить пакет anonsftp

```
[root@server-alt10 ~]# apt-get update_
```

```
[root@server-alt10 ~]# apt-get install anonftp
Reading Package Lists... Done
Building Dependency Tree... Done
The following NEW packages will be installed:
```

- 4.3. На сервере server-alt10 создать пользователей admin_ftp и user_ftp, задать пароли и включить пользователя admin_ftp в группу ftpadmin

```
[root@server-alt10 ~]# useradd admin_ftp
[root@server-alt10 ~]# passwd admin_ftp
```

```
[root@server-alt10 ~]# usermod -aG ftpadmin admin_ftp
[root@server-alt10 ~]#
```

```
[root@server-alt10 ~]# useradd user_ftp
[root@server-alt10 ~]# passwd user_ftp
```

- 4.4. Создать в каталоге /var/ftp каталоги, установить права доступа, а также владельцев и владельцев-групп:

- 4.4.1. /var/ftp/public. - каталог для размещения общедоступных файлов.

Для него установить права доступа 2775. При этом анонимным пользователям FTP-сервера будет предоставлен доступ на чтение к файлам, находящимся в каталоге. Владелец каталога - root. Группа-владелец - ftpadmin.

```
[root@server-alt10 ~]# mkdir /var/ftp/public
[root@server-alt10 ~]# chgrp ftpadmin /var/ftp/public
[root@server-alt10 ~]# chmod -R 2775 /var/ftp/public
[root@server-alt10 ~]# ls -la /var/ftp/public
total 8
drwxrwsr-x 2 root ftpadmin 4096 Apr  5 19:47 .
drwxrwsr-x 3 root ftpadmin 4096 Apr  5 19:47 ..
```

- 4.4.2. /var/ftp/incoming - каталог с разрешением анонимным

пользователям сервера доступа на запись. Права доступа 3773 (владелец - admin_ftp, группа-владелец - ftpadmin). Анонимным пользователям предоставляется право записи в этот каталог, без возможности просмотра его содержимого.

```
[root@server-alt10 ~]# mkdir /var/ftp/incoming
[root@server-alt10 ~]# chgrp ftpadmin /var/ftp/incoming
[root@server-alt10 ~]# chmod -R 3773 /var/ftp/incoming
[root@server-alt10 ~]# ls -la /var/ftp/incoming
total 8
drwxrws-wt 2 root ftpadmin 4096 Apr  5 19:49 .
drwxrwsr-x 4 root ftpadmin 4096 Apr  5 19:49 ..
```

5. Настроить на сервере server-alt10 FTP-сервер vsftpd

5.1. Установить правила для анонимного и авторизованного доступа.

Внести изменения в файле конфигурации /etc/vsftpd/conf

```
root@server-alt10 ~]# nano /etc/vsftpd/conf
```

Изменим содержание файла конфигурации

```
GNU nano 7.2 /etc/vsftpd/conf
# For anonymous
#listen=YES
#anonymous_enable=YES
#anon_root=/var/ftp
#anon_upload_enable=NO
#anon_mkdir_write_enable=NO
#anon_umask=022
#anon_max_rate=0
#anon_other_write_enable=NO
#local_enable=NO
```

```
# For authorised
listen=YES
anonymous_enable=YES
local_enable=YES
write_enable=YES
local_umask=022
chroot_local_user=YES
allow_writeable_chroot=YES
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
local_max_rate=1000000
local_root=/var/ftp
```

```
[root@server-alt10 ~]# touch /etc/vsftpd.userlist
[root@server-alt10 ~]# chmod 600 /etc/vsftpd.userlist
[root@server-alt10 ~]# chown root:root /etc/vsftpd.userlist
```

```
[root@server-alt10 ~]# nano /etc/vsftpd.userlist
```

```
GNU nano 7.2 /etc/vsftpd.userlist
user_ftp
admin_ftp_
```

```

nopriv_user=novsftpd
anonymous_enable=YES
no_anon_password=YES
local_enable=YES
write_enable=YES
anon_upload_enable=YES
anon_mkdir_write_enable=YES
nopriv_user=novsftpd
ftpd_banner=
```

Не работает сервис vsftpd, поэтому настроим unit-файл

```
GNU nano 7.2 /etc/systemd/system/vsftpd.service
[Unit]
Description=vsftpd FTP server
After=network.target

[Service]
Type=simple
ExecStart=/usr/sbin/vsftpd /etc/vsftpd.conf
Restart=on-failure

[Install]
WantedBy=multi-user.target_
```

```
[root@server-alt10 ~]# systemctl daemon-reload
[root@server-alt10 ~]# systemctl enable --now vsftpd
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service ? /etc/systemd/system/vsftpd.service.
```

6. Настроить демон службы xinetd и перезапустить службу

```
[root@server-alt10 ~]# nano /etc/xinetd.d/vsftpd_
```

```
GNU nano 7.2 /etc/xinetd.d/vsftpd
default: off
description: The vsftpd FTP server.
service ftp
{
    disable           = no
    socket_type       = stream
    protocol          = tcp
    wait              = no
    user              = root
    nice               = 10
    rlimit_as         = 200M
    server             = /usr/sbin/vsftpd
#    server_args      =
    only_from         = 0/0
}
```

```
[root@server-alt10 ~]# nano /etc/xinetd.conf
```

```
GNU nano 7.2 /etc/xinetd.conf
#
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

defaults
{
    log_type = SYSLOG authpriv info
    log_on_success = PID HOST DURATION
    log_on_failure = HOST
    instances = 100
    per_source = 5
#    only_from = 127.0.0.1
}

includedir /etc/xinetd.d
```

```
[root@server-alt10 ~]# systemctl restart xinetd
```

7. Установить запуск сервиса xinetd при загрузке системы

```
[root@server-alt10 ~]# chkconfig xinetd on
Note: Forwarding request to 'systemctl enable xinetd.service'.
Synchronizing state of xinetd.service with SysV service script with /lib/systemd
/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable xinetd
```

8. Установить программы FTP-клиентов

8.1. Установить на рабочей станции ws1-alt10 FTP-клиентов ftp и FileZilla

```
[root@ws1-alt10 ~]# apt-get update
Получено: 1 http://mirror.yandex.ru p10/branch/x86_64 release [4215B]
Получено: 2 http://mirror.yandex.ru p10/branch/x86_64-i586 release [1665B]
Получено: 3 http://mirror.yandex.ru p10/branch/noarch release [2836B]
Получено 8716B за 0s (65,6kB/s).
Найдено http://mirror.yandex.ru p10/branch/x86_64/classic pkglist
Найдено http://mirror.yandex.ru p10/branch/x86_64/classic release
```

```
[root@ws1-alt10 ~]# apt-get install ftp
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие НОВЫЕ пакеты будут установлены:
  ftp
0 будет обновлено, 1 новых установлено, 0 пакетов будет удалено и 0 не будет обн
овлено.
```

```
[root@ws1-alt10 ~]# apt-get install filezilla
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие дополнительные пакеты будут установлены:
  libfilezilla libpugixml libwxBase3.0 libwxGTK3.0
```

9. Подключиться к серверу FTP в консольном режиме

9.1. Подключиться к FTP- серверу в режиме анонимного и авторизованного доступа

В режиме анонимного доступа

```
[root@ws1-alt10 ~]# ftp 192.168.100.100
Connected to 192.168.100.100 (192.168.100.100).
220 Welcome to blah FTP service.
Name (192.168.100.100:admin_ws): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
ftp> pwd
257 "/" is the current directory
ftp> ls
227 Entering Passive Mode (192,168,100,100,192,46).
150 Here comes the directory listing.
drwxrws-wt  2 ftp      ftp          4096 Apr 05 16:49 incoming
drwxrwsr-x  2 ftp      ftp          4096 Apr 05 16:47 public
226 Directory send OK.
```

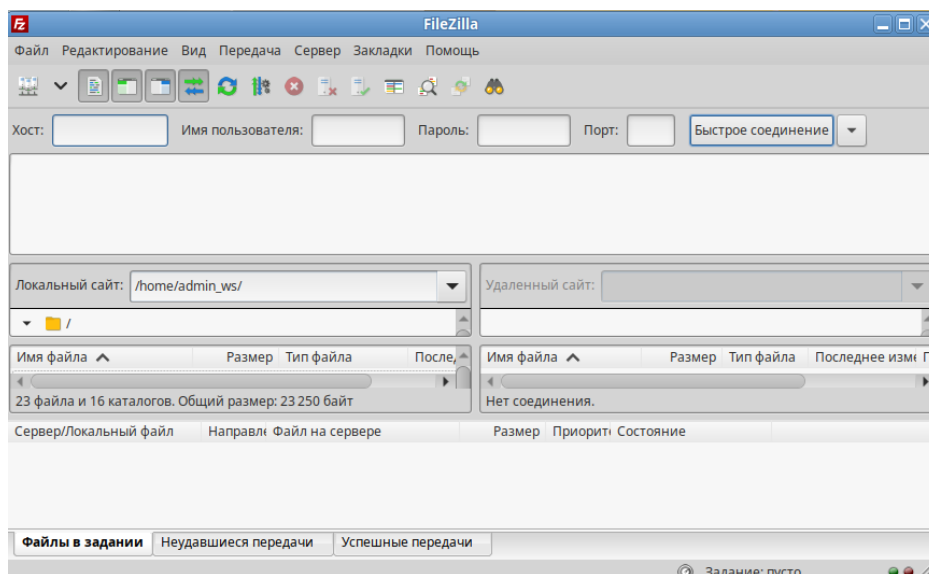
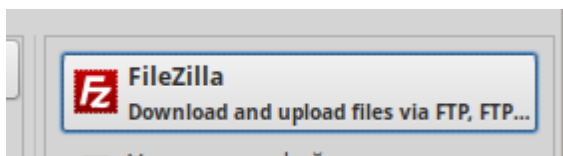
В режиме авторизованного доступа

```
[root@ws1-alt10 ~]# ftp 192.168.100.100
Connected to 192.168.100.100 (192.168.100.100).
220 Welcome to blah FTP service.
Name (192.168.100.100:admin_ws): anonymous
530 Permission denied.
Login failed.
ftp> exit
221 Goodbye.
[root@ws1-alt10 ~]# ftp 192.168.100.100
Connected to 192.168.100.100 (192.168.100.100).
220 Welcome to blah FTP service.
Name (192.168.100.100:admin_ws): user_ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
ftp> pwd
257 "/" is the current directory
ftp> ls
227 Entering Passive Mode (192,168,100,100,253,199).
150 Here comes the directory listing.
drwxrws-wt  2 ftp      ftp      4096 Apr 05 16:49 incoming
drwxrwsr-x  2 ftp      ftp      4096 Apr 05 16:47 public
226 Directory send OK.
```

10. Подключиться к серверу FTP в графическом режим

10.1. Выполнить команды для скачивания и загрузки файлов на FTP-сервер с помощью программы FileZilla



Контрольные вопросы

1. Для чего предназначен протокол FTP?

Протокол FTP (File Transfer Protocol) предназначен для:

- Передачи файлов между компьютерами по сети: Это его основная и главная функция. FTP позволяет передавать файлы любого типа (текстовые, бинарные, изображения, архивы и т.д.) между клиентом и сервером.
- Загрузки файлов на сервер (upload): Клиент может загружать файлы с локального компьютера на FTP-сервер. Это часто используется для загрузки веб-сайтов на хостинг, обмена файлами между пользователями или создания резервных копий.
- Скачивания файлов с сервера (download): Клиент может скачивать файлы с FTP-сервера на локальный компьютер. Это используется для получения файлов, размещенных на сервере, например, программного обеспечения, документации или мультимедийного контента.
- Управления файлами на сервере: FTP позволяет выполнять различные операции с файлами и каталогами на сервере, такие как создание каталогов, удаление файлов и каталогов, переименование файлов и каталогов, изменение прав доступа.
- Организации общего доступа к файлам: FTP-сервер может быть настроен для предоставления общего доступа к определенным файлам или каталогам для пользователей, имеющих соответствующие учетные данные.

2. Перечислите этапы FTP-соединения.

FTP-соединение обычно включает в себя следующие этапы:

1. Установление управляющего соединения (Control Connection):
 - Клиент устанавливает TCP-соединение с FTP-сервером на порту 21.

- Это соединение используется для отправки команд и получения ответов между клиентом и сервером (например, для аутентификации, навигации по каталогам, запроса списка файлов).

2. Аутентификация:

- Клиент отправляет серверу имя пользователя (USER) и пароль (PASS).
- Сервер проверяет учетные данные и авторизует клиента.

3. Установка режима передачи (Active или Passive):

- Активный режим (ACTIVE): Клиент сообщает серверу свой IP-адрес и порт, на котором он будет ожидать соединение для передачи данных. Сервер устанавливает TCP-соединение с клиентом на этот порт для передачи данных.
- Пассивный режим (PASSIVE): Клиент запрашивает у сервера порт для передачи данных. Сервер выделяет порт и сообщает его клиенту. Клиент устанавливает TCP-соединение с сервером на этот порт для передачи данных.

4. Передача данных (Data Connection):

- После установки режима передачи клиент отправляет серверу команду на передачу данных (например, RETR для скачивания, STOR для загрузки, LIST для получения списка файлов).
- Сервер устанавливает (или уже установил в зависимости от режима) соединение для передачи данных и передает запрошенные данные.

5. Завершение передачи данных:

- После завершения передачи данных сервер закрывает соединение для передачи данных.

6. Разрыв соединения (Control Connection):

- После завершения всех необходимых операций клиент отправляет серверу команду QUIT.

- Сервер закрывает управляющее соединение.

Важно отметить: Активный режим может вызывать проблемы с брандмауэрами, так как сервер пытается установить соединение с клиентом. Пассивный режим обычно предпочтительнее, так как клиент устанавливает все соединения.

3. Какова особенность сервера vsftpd?

vsftpd (Very Secure FTP Daemon) - это FTP-сервер, который отличается следующими особенностями:

- **Безопасность:** Главный акцент сделан на безопасность. vsftpd разработан с учетом принципов минимальных привилегий и использует различные механизмы защиты для предотвращения атак. Он считается одним из самых безопасных FTP-серверов.
- **Производительность:** vsftpd оптимизирован для высокой производительности и масштабируемости. Он может обрабатывать большое количество одновременных соединений.
- **Простота:** Несмотря на акцент на безопасность, vsftpd относительно прост в настройке и использовании. Конфигурационный файл достаточно понятен.
- **Поддержка виртуальных пользователей:** vsftpd поддерживает создание виртуальных пользователей, которые не имеют системных учетных записей. Это позволяет предоставлять доступ к FTP-серверу пользователям, не имеющим учетных записей в операционной системе.
- **Поддержка SSL/TLS:** vsftpd поддерживает шифрование соединений с использованием SSL/TLS, что обеспечивает защиту передаваемых данных от перехвата.
- **Ограничение доступа:** vsftpd позволяет настраивать различные ограничения доступа для пользователей, такие как ограничение скорости передачи данных, ограничение количества одновременных соединений, ограничение доступа к определенным каталогам.

- Поддержка IPv6: vsftpd поддерживает протокол IPv6.
- Интеграция с PAM: vsftpd может использовать PAM (Pluggable Authentication Modules) для аутентификации пользователей, что позволяет интегрировать его с различными системами аутентификации.
- Ориентация на Linux/Unix: vsftpd изначально разрабатывался для Linux и Unix-подобных операционных систем, хотя существуют порты и на другие платформы.

В целом, vsftpd – это надежный, безопасный и производительный FTP-сервер, который часто используется в Linux-системах для предоставления доступа к файлам по протоколу FTP. Его безопасность и простота делают его популярным выбором для многих администраторов.