Лабораторная работа №2
«Основные сетевые утилиты»

1. Теоретическая часть

1.1. FTP-сервер

FTP (File Transport Protocol) – протокол передачи файлов по сети прикладного уровня модели OSI.

Протокол появился в 1971 году и, несмотря на возраст, активно используется повсеместно.

FTP-сервер представляет собой хранилище файлов, который по запросу из сети осуществляет приём или передачу файлов.

Репозиторий (от англ. repository — хранилище) — место, где хранятся и поддерживаются какие-либо данные.

Именно на FTP-репозитории была впервые выложена первая версия ядра Linux. Расположение репозитория на одном сервере позволяет пользователям локальной или глобальной сети обращаться к ней, тем самым не вынуждая хранить данные у себя на локальной машине и легко делиться ими с другими.

В качестве FTP-сервера предлагается программа **vsftpd** (**V**ery **S**ecure **FTP** **D**aemon), распространяемая под лицензией GPL. Её установить можно с официальных репозиториев Astra Linux менеджером пакетов **apt**. Делается это следующей командой:

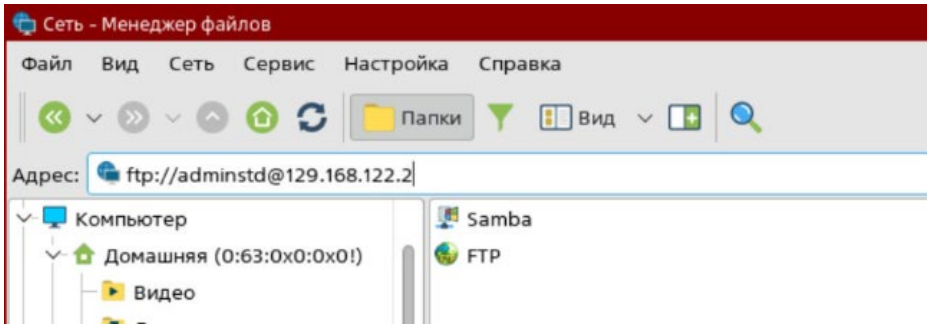
```
sudo apt install vsftpd
```

Для настройки необходимо с правами суперпользователя отредактировать конфигурационный файл **/etc/vsftpd.conf**. Некоторые параметры должны иметь следующий вид:

```
listen=yes
listen_ipv6=no
anonymous_enable=YES
```

После каждого изменения конфигурационного файла необходимо перезапустить службу **vsftpd**.

Проверить работу FTP-сервера можно с помощью менеджера файла, как показано на рисунке ниже. В адресной строке указывается протокол ftp, затем имя пользователя, который имеет доступ к репозиторию, IP-адрес сервера. Будет предложено ввести пароль указанного пользователя.



1.2. SMB-сервер

SMB (сокр. от англ. Server Message Block) — сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам.

Samba — пакет программ, которые позволяют обращаться к сетевым дискам и принтерам на различных операционных системах по протоколу SMB. Работает через порт 445.

Для установки Samba используется команда

```
sudo apt install samba
```

В качестве примера создадим общую папку. Для этого командой

```
mkdir /srv/share
```

создадим папку. Изменим права доступа к этой папке

```
sudo chown nobody:nogroup /srv/share
sudo chmod 777 /srv/share
```

Далее в конец файла **/etc/samba/smb.conf** необходимо добавить следующие строки:

```
map to guest = Bad User
[share]
  comment = <Произвольный комментарий>
  guest ok = yes
  force user = nobody
  force group = nogroup
  path = /srv/share
  read only = no
```

После сохранения файла проверяем установку параметров командой **testparm.** Осуществляем перезагрузку командой **sudo systemctl restart smbd**.

Работа с общими папками происходит с использованием протокола CIFS (**C**ommon **I**nternet **F**ile **S**ystem). Поэтому стоит убедиться, что в системе установлен пакет **cifs-utils**. Её использование определяется следующим синтаксисом:

```
$ mount -t cifs <папка на сервере> <во что монтируем> <-o опции>
```

То есть, чтобы клиент мог подключиться к общей папке, ему необходимо выполнить следующую команду:

```
sudo mount -t cifs //A.B.C.D/share /mnt/smb -o users,sec=none
```

Программа **mount** используется для монтирования USB-устройств, дисков, сетевых папок и т.д. Ключ **-t** указывает тип файловой системы **cifs**. После символов // пишется IP-адрес SMB-сервера, название общей папки. Всё это монтируется в папку **/mnt/smb**, а ключом **–o** указываются опции **users** (папка для всех пользователей) и **sec** (отвечает за безопасность).

После подключения в менеджере файлов во вкладке **Сеть/Samba** должна появиться сетевая папка с именем сервера, где и будет лежать общая папка.

1.3. Файловая система NFS

NFS (сокращение от **N**etwork **F**ile **S**ystem, Сетевая Файловая Система) - сервис, обеспечивающий общий доступ к файлам и каталогам систем *nix / Linux. Файловая система NFS позволяет монтировать удалённые разделяемые файлы подобно локальным.

Для установки NFS необходимо выполнить команды.

На сервере:

```
sudo apt install nfs-kernel-server
```

На клиенте:

```
sudo apt install nfs-common
```

После установки утилит на сервере необходимо создать и настроить директорию, которая будет доступна для монтирования с других устройств. Для этого создадим её.

```
sudo mkdir /srv/nfsshare
sudo chmod 777 /srv/nfsshare
sudo chown nobody:nogroup /srv/nfsshare
```

Для конфигурации NFS необходимо отредактировать файл /etc/exports. Для подключения директории в него необходимо добавить строку вида:

```
directory client(options)
```

Где:

- **directory** — папка, к которой нужно открыть доступ по сети.
- **client** — IP-адрес машины или подсети, которой будет доступна эта папка
- **options** — опции, используемые в настройках.

В качестве опций возможно указать:

- rw — чтение запись (может принимать значение ro – только чтение);

- no_root_squash — по умолчанию в общих ресурсах NFS пользователь root становится обычным пользователем nfsnobody. Таким образом, владельцем всех файлов, созданных root, становится nfsnobody, что предотвращает загрузку на сервер программ с установленным битом setuid. Использование параметра no_root_squash не рекомендуется, так как потенциально создает угрозы безопасности, связанные с возможностью удаленного внедрения в файловую систему вредоносного ПО.
- nohide — NFS автоматически не показывает нелокальные ресурсы (например, примонтированные с помощью mount –bind), эта опция включает отображение таких ресурсов;
- sync — синхронный режим доступа (может принимать обратное значение- async). Значение sync указывает, что сервер должен отвечать на запросы только после записи на диск изменений, выполненных этими запросами. Параметр async указывает серверу не ждать записи информации на диск, что повышает производительность, но понижает надежность, т.к. в случае обрыва соединения или отказа оборудования возможна потеря данных.
- noaccess — запрещает доступ к указанной директории. Применяется, если доступ к определенной директории выдан всем пользователям сети , и необходимо ограничить доступ для некоторых пользователей.
- all_squash — подразумевает, что все подключения будут выполнятся от анонимного пользователя;
- subtree_check (no_subtree_check)- в некоторых случаях приходится экспортировать не весь раздел, а лишь его часть. При этом сервер NFS должен выполнять дополнительную проверку обращений клиентов, чтобы убедиться в том, что они предпринимают попытку доступа лишь к файлам, находящимся в соответствующих подкаталогах. Такой

контроль поддерева (subtree checks) несколько замедляет взаимодействие с клиентами, но если отказаться от него, могут возникнуть проблемы с безопасностью системы. Отменить контроль поддерева можно с помощью опции no_subtree_check. Опция subtree_check, включающая такой контроль, предполагается по умолчанию. Контроль поддерева можно не выполнять в том случае, если экспортируемый каталог совпадает с разделом диска.

- anonuid=1000 — привязывает анонимного пользователя к «местному» пользователю;
- anongid=1000 — привязывает анонимного пользователя к группе «местного» пользователя.

Например, строка конфигурационного файла может выглядеть таким образом:

```
/srv/nfsshare 192.168.122.2(rw,nohide,all_squash,anonuid=1000,anongid=1000,no_subtree_check)
```

После внесения изменений для того, чтобы они вступили в силу, нужно выполнить команду

```
sudo exportfs -ra
```

На клиенте необходимо примонтировать настроенный ресурс. Для получения списка доступных ресурсов воспользуйтесь командой

```
sudo showmount -e 192.168.122.2
```

где 192.168.122.2 – адрес сервера NFS.

Чтобы примонтировать каталог возможно воспользоваться командой mount

```
sudo mount 192.168.122.2:/srv/nfsshare /mnt/nfs
```

1.4. NTP-сервер

NTP (англ. Network Time Protocol — протокол сетевого времени) — сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей.

Для синхронизации времени в системах GNU/Linux используется демон **ntpd** (**N**etwork **T**ime **P**rotocol **d**aemon). Для его установки применяется команда

```
sudo apt install ntp
```

Принцип работы NTP основан на использовании иерархии серверов, которая обеспечивает распределение точного времени по всей сети. Уровни этой иерархии называются стратами (англ. strata). Высший уровень 0 представляет источники времени такие как атомные часы. Следующий уровень 1 — это серверы, которые получают точное время от нулевого уровня и сами могут служить источником времени для серверов следующего уровня 2. Этот процесс продолжается до достижения конечных клиентских устройств.

Иерархическая структура протокола NTP построена с учетом отказоустойчивости и избыточности. В случае потери соединения с вышестоящими серверами NTP резервные серверы берут процесс синхронизации на себя. За счёт избыточности обеспечивается постоянная доступность NTP-серверов. Синхронизируясь с несколькими серверами, NTP использует данные всех источников, чтобы рассчитать наиболее точное время.

В качестве примера рассмотрим локальную сеть, состоящую из NTP-сервера и его клиента и изолированную от глобальной сети Интернет. По умолчанию сервер настроен на получение точного времени от прописанных в конфигурационном файле вышестоящих серверов. Однако при отсутствии связи с сетью Интернет, сервер будет высылать по запросу своё системное время.

Конфигурационный файл имеет путь **/etc/ntpsec/ntp.conf**. Он содержит начальные настройки и примеры конфигурирования для различных задач. Рекомендуется сделать резервное копирование файла с помощью команды

```
sudo cp /etc/ntpsec/ntp.conf /etc/ntpsec/ntp.conf.orig
```

Для понимания процесса настройки сервера, удалим конфигурационный файл командой **sudo rm /etc/ntp.conf** и в редакторе создадим новый командой

```
sudo nano /etc/ntpsec/ntp.conf
```

В пустой файл впишем следующую строку

```
server 127.127.1.0 prefer
```

Директива **server** указывает, к какому серверу необходимо подключиться для получения точного времени. IP-адрес 127.127.1.0 – это адрес, по которому сервер получает своё системное время, которое и будет отправлять по запросу клиенту. Опция **prefer** в данном случае указывается обязательно, так как серверу не нравится факт использования своего времени из-за высокой вероятности рассинхронизации с точным мировым временем.

После внесения изменений в конфигурационный файл необходимо перезагрузить службу командой **sudo systemctl restart ntp**. Проверить текущее состояние службы можно командой **status** вместо **restart**.

В качестве теста запустим эмулятор терминала на клиенте и введём команду **sudo ntpdate A.B.C.D**, где A.B.C.D – IP-адрес локального NTP-сервера. В случае успеха будет показано, насколько установленное на клиенте время отличается от времени сервера.

1.5. Основы безопасности локальной вычислительной сети

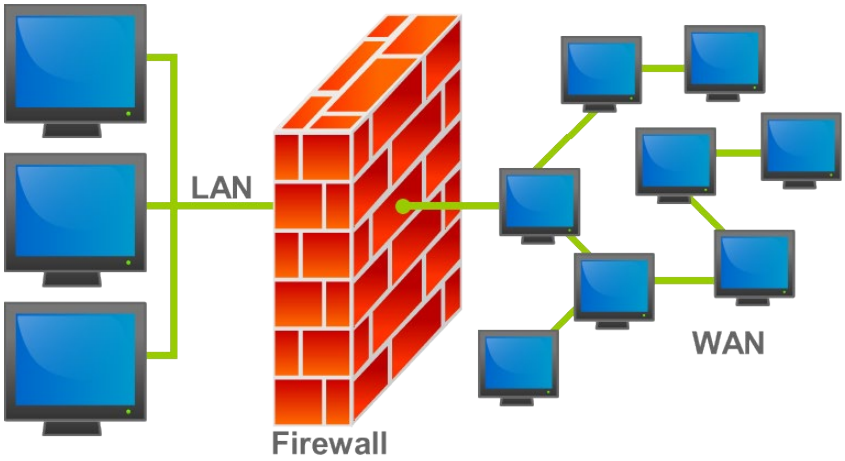
Локальная вычислительная сеть, в каком бы виде она ни была (домашняя или корпоративная), всегда подвержена угрозам как снаружи (из внешней глобальной сети), так и изнутри (со стороны сотрудников или подключившегося к ЛВС злоумышленника).

В обязанности сетевого администратора входит разграничение прав доступа к различным ресурсам ЛВС, а также установление политики доступа к глобальной сети Интернет (если сама сеть физически подключена к нему).

Существует множество методов защиты, как аппаратных, так и программных.

Межсетевой экран (Брандмауэр, Firewall) – средство межсетевой защиты, которое позволяет разделить общую сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов через границу из одной части общей сети в другую.

Как правило, граница проводится между корпоративной (локальной) сетью организации и глобальной сетью. МЭ пропускает через себя весь трафик, принимая для каждого пакета решение – пропускать его или отбросить.



В операционных системах GNU/Linux используется встроенное в ядро Linux межсетевой экран **Netfilter**. Для его конфигурирования применяется утилита **ufw** (Uncomplicated Firewall, с англ. — «незамысловатый межсетевой экран»).

Основные команды **ufw** для командной строки:

Команда	Описание
ufw enable	Включить firewall, т.е. перевести его в активное состояние
ufw status	Просмотр текущего состояния
ufw status verbose	Подробная информация о состоянии
ufw app list	Вывести список известных правил для приложений
ufw allow ***имя_приложения/порт***	Добавить разрешающее правило для приложения, например **ufw allow SSH или ufw allow 22**
ufw deny ***имя_приложения/порт***	Добавить запрещающее правило для приложения, например **ufw deny SSH или ufw deny 22**
ufw show added	Просмотреть добавленные пользователем правила

ufw logging [on|off]	Включить|выключить запись логов. Прочитать их возможно с помощью dmesg
ufw reset	Восстановить правила и состояние "по умолчанию". Так как "по умолчанию" сервис выключен, после этой команды его нужно включить: **ufw enable**
ufw disable	Отключить firewall

Примечание: более подробно примеры использования ufw смотреть в man.

Обратите внимание, после перезагрузки значения, установленные пользователем сохраняются.

2. Практическая часть

2.1. Задание 1

2.1.1. На сервере создайте локальный FTP-репозиторий и загрузите на него файл, содержащий в названии ваши ФИО.

2.1.2. Выгрузите файл из созданного репозитория на машину workstation.

2.1.3. Создайте на сервере общую папку smb и примонтируйте её на машине Node1 в директорию /mnt/ваши_инициалы_smb. (Например, /mnt/sabsmb)

2.1.4. Создайте на сервере общую папку nfs и примонтируйте её на машине Node1 в директорию /mnt/ваши_инициалы_nfs. (Например, /mnt/sabnfs)

2.2. Задание 2

2.2.1. Настройте межсетевой экран перед включением. Для этого добавьте правило, разрешающее подключение к серверу по SSH.

2.2.2. Включите встроенный межсетевой экран на сервере и выполните сброс текущего состояния.

2.2.3. Проверьте доступность nfs и smb директорий. Настройте к ним доступ. Для этого укажите разрешающее правило, используя название службы у nfs и порт у smb.

2.2.4. Выключите межсетевой экран.

2.3. Задание 3.

2.3.1. На node1, поменяйте дату и время на 01.01.1970 и 18:12. Для этого воспользуйтесь командой date. Формат записи выясните, используя утилиту man.

2.3.2. Синхронизируйте время Server и node1 по сети, установив NTP-сервер на машину Server и добавив её в автозагрузку.

Контрольные вопросы

1. Как работает Firewall?
2. Какие существуют способы передачи файлов по сети?