Учреждение образования

«Белорусский Государственный Технологический Университет»

**Отчет по лабораторной работе №3, 3.1**

**Подготовка виртуальных машин к развертыванию облака OpenNebula**

по дисциплине «Облачные технологии»

Выполнила:

Студентка 4 курса 2-2 спец. ИСиТ

Кохнюк Александра

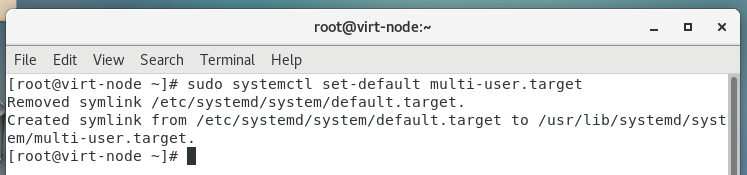
Проверила:

Харланович А.В.

Минск 2024

**Создание ВМ с ОС Linux CentOS Server для главного узла облака OpenNebula**

**Отключение GUI (X-Windows) при загрузке CentOS.** Отключить запуск X-ов при старте системы можно выполнив команду



Проверяем



Перезагружаемся без GUI.

**$ sudo reboot**



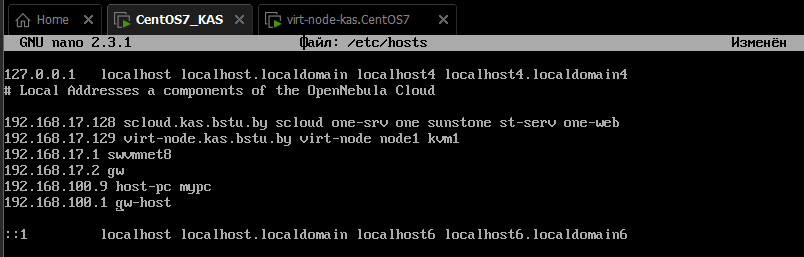
Вернуть обратно запуск графической оболочки можно с помощью команды:

**$ sudo systemctl set-default graphical.target**

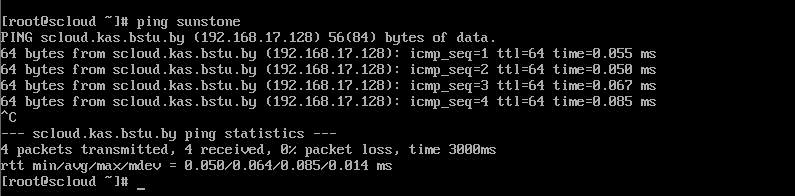
**Внесение имен узлов облака в файл /etc/hosts на управляющем узле**

|  |  |  |  |
| --- | --- | --- | --- |
| № п.п | Имя узла | IP-адрес узла | Назначение узла |
| 1 | **scloud.sdk.bstu.by**  one-serv | 192.168.17.128 | Сервер OpenNebula |
| 2 | **sunstone**  st-serv  one-web | 192.168.17.128 | Web-сервер Sunstone управления облаком |
| 3 | **virt-node.sdk.bstu.by**  virt-node1  node1  kvm1 | 192.168.17.129 | Сервер виртуализации |
| 4 | **swvmnet8** | 192.168.17.1 | Виртуальный коммутатор VmNet8 |
| 5 | **gw** | 192.168.17.2 | Шлюз виртуальной сети облака |
| 6 | dns-srv | 192.168.17.2 | Сервер DNS |
| 7 | host-pc  mypc | 192.168.100.9 | Хозяйская машина |
| 8 | **gw-host** | 192.168.100.1 | Шлюз хозяйской машины |

На управляющем узле scloud откроем файл /etc/hosts и внесем в него следующие записи, после записей 127.0.0.1, но до адресов IPv6:



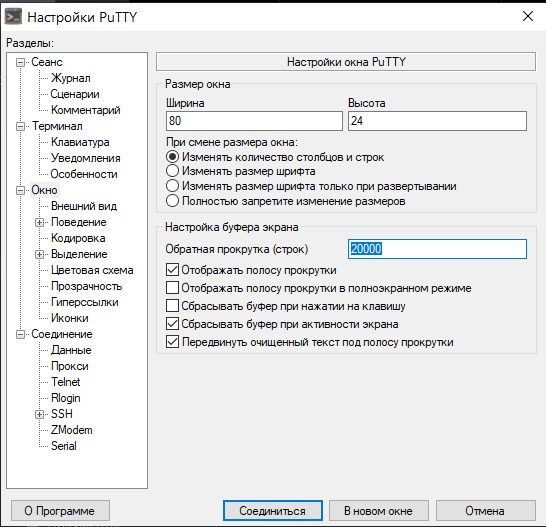
Проверить правильность назначения имен можно с помощью команды **ping**:



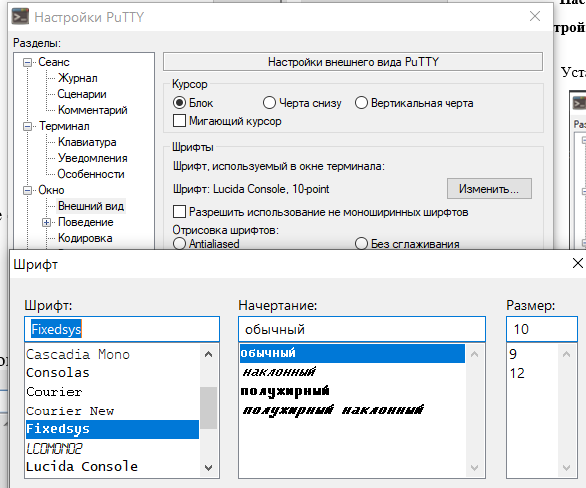
Содержание отредактированного файла /etc/hosts в дальнейшем необходимо будет скопировать на все остальные узлы инфраструктуры создаваемого облака, включая хостовую машину.

**Настройка Putty**

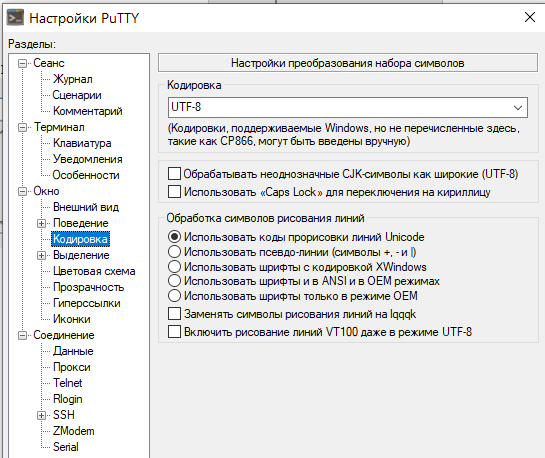
1. Устанавливаем размер буфера прокрутки экрана 20000



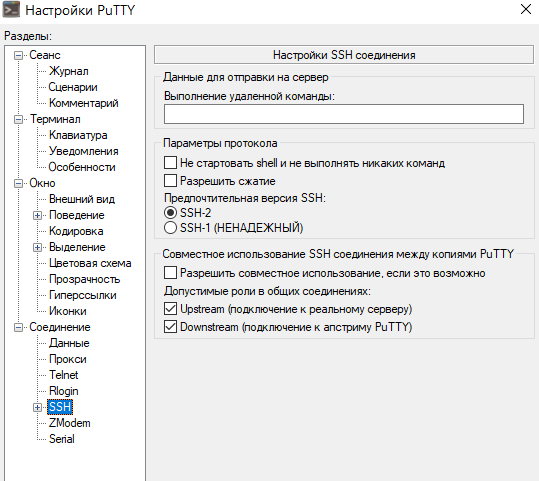
1. Установливаем шрифт Fixedsys 10-point, для чего нажимаем кнопку Change



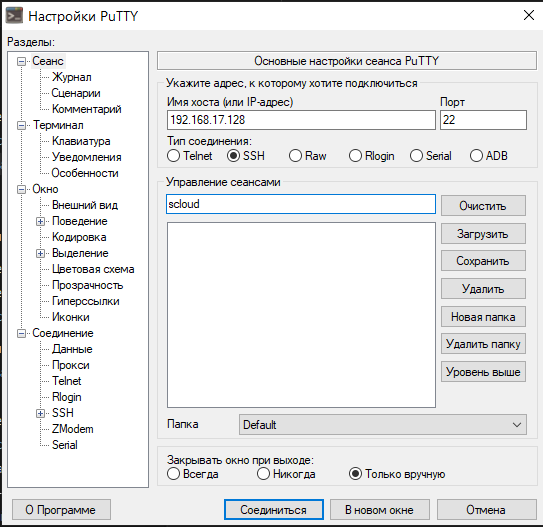
1. Кодировка. UTF-8: Универсальная кодировка символов, которая поддерживает множество языков и символов Unicode. Выбор правильной кодировки символов в Putty важен для правильного отображения текста на удаленной системе и предотвращения проблем с отображением символов



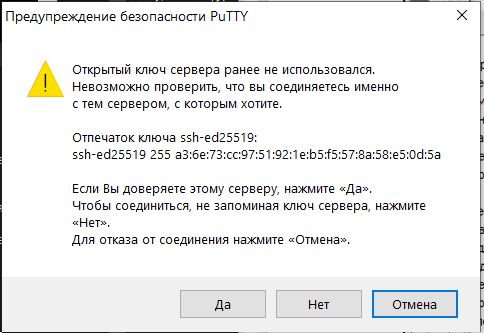
1. SSH. Выбрать версию 2. SSH позволяет пользователям безопасно взаимодействовать с удаленными системами, передавая команды и получая ответы через шифрованное соединение. Он обеспечивает шифрование трафика и аутентификацию, что делает его надежным средством удаленного доступа



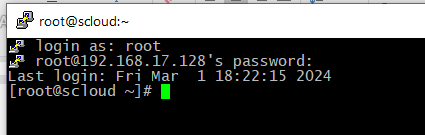
**Подключение:** указываем ip адрес и номер порта:



После запроса соединения появится окно, сообщающее о том, что для данного сервера в реестре отсутствуют ключи шифрования. Здесь с согласия предлагается использовать ключи шифрования, предоставляемые самой программой

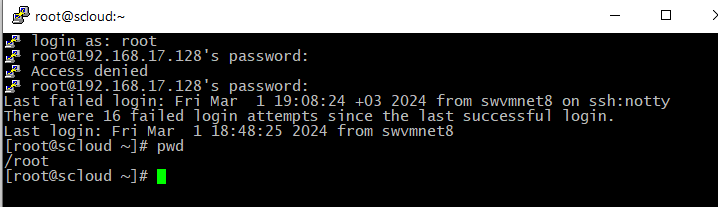


Аутентификация на машине центрального узла происходит при помощи ввода логина и пароля:

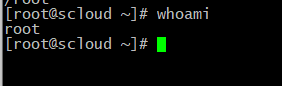


**Работа со службой SSH**

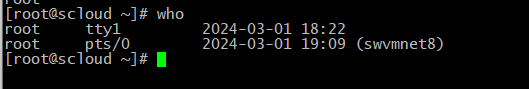
Теперь, войдя в систему, можно посмотреть имя (полный путь) текущего каталога при помощи команды **pwd**



Чтобы просмотреть имя текущего пользователя, под которым был осуществлен вход в систему, можно ввести команду **whoami**

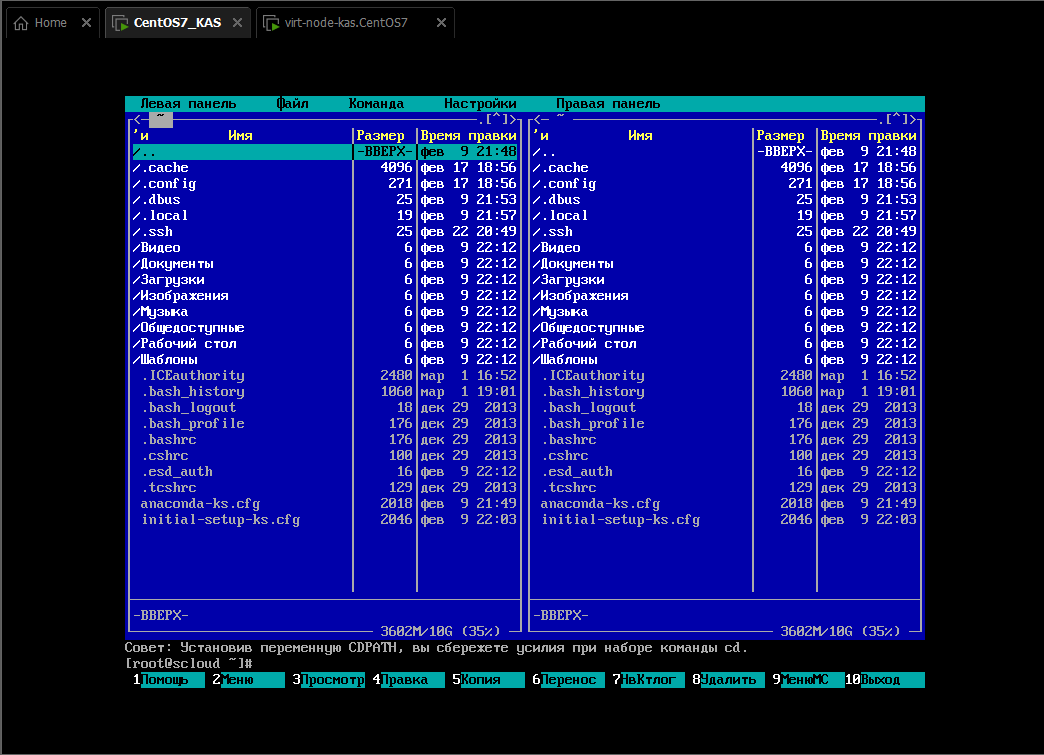


Команда **who** в свою очередь выведет имена всех пользователей, находящихся в системе. Результат команды **who** – это вывод имен пользователей, а также дата и время их входа и название терминала, с которого был осуществлен вход.



**Midnight Commander**

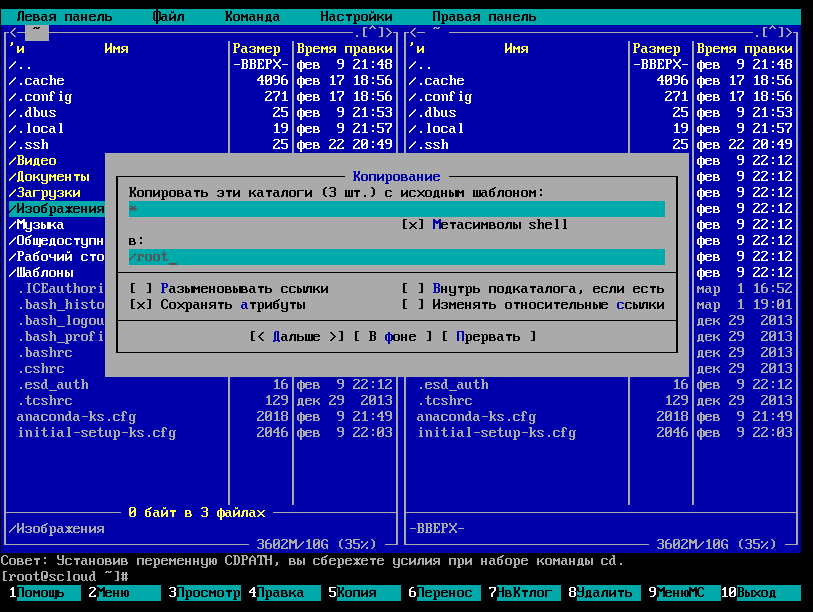
Для перехода в оболочку mc используется одноименная **команда mc.**



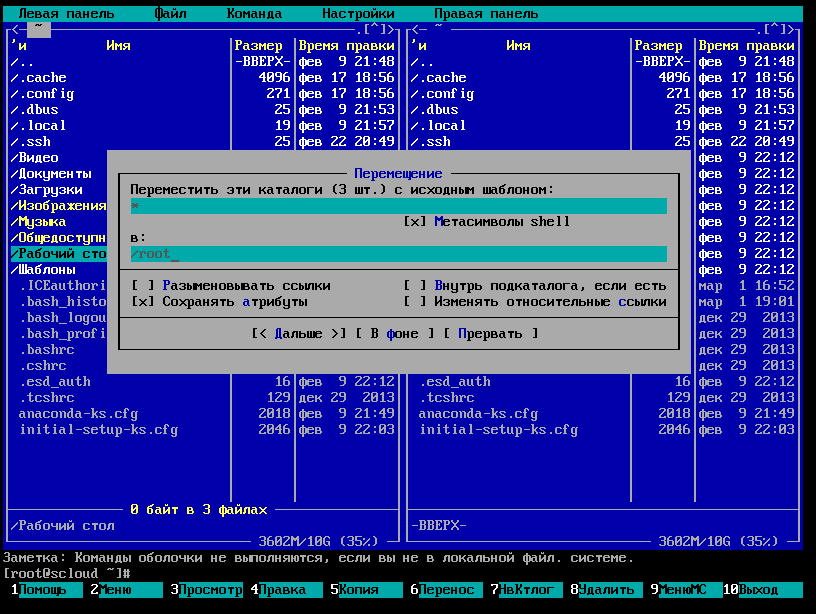
Множественное выделение файлов или каталогов в mc происходит при помощи **клавиши Insert (подсвечиваются желтым цветом)**



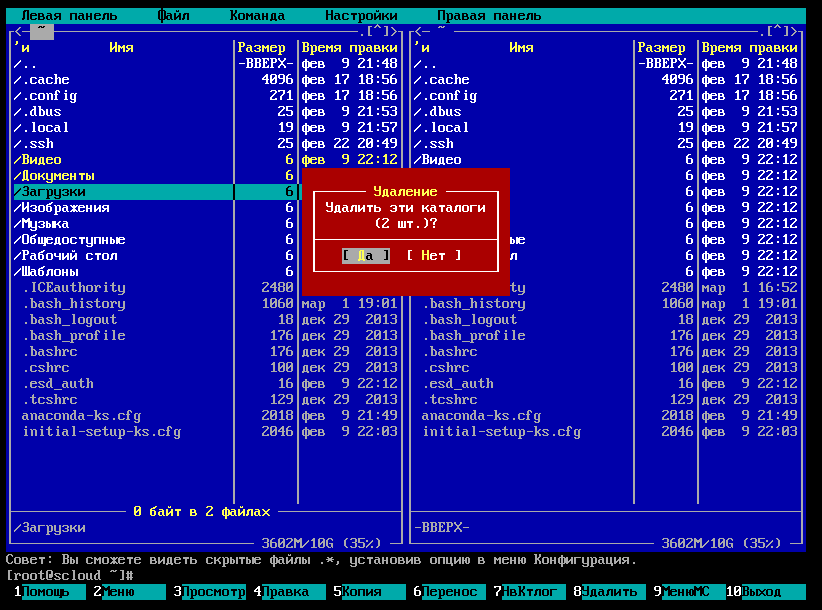
Копирование файлов и директорий осуществляется при помощи **клавиши F5**



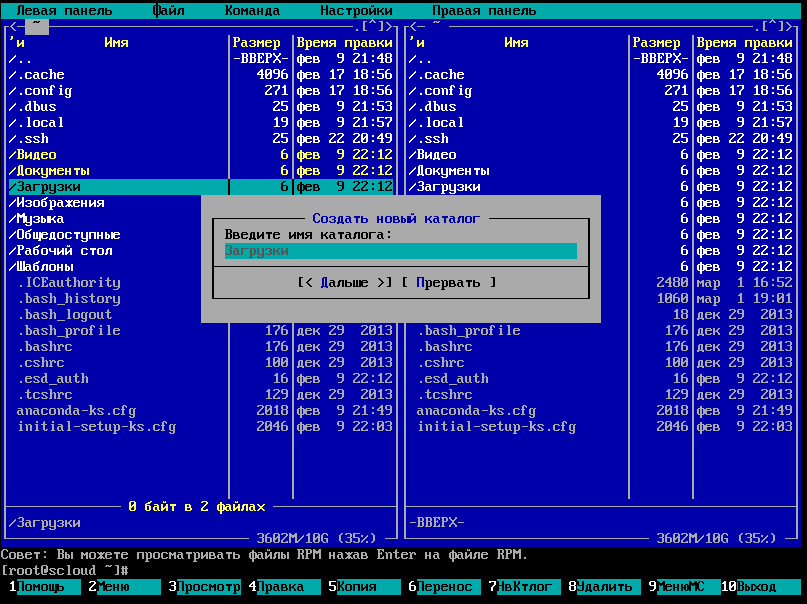
Перемещение файлов или директорий производится нажатием **клавиши F6**



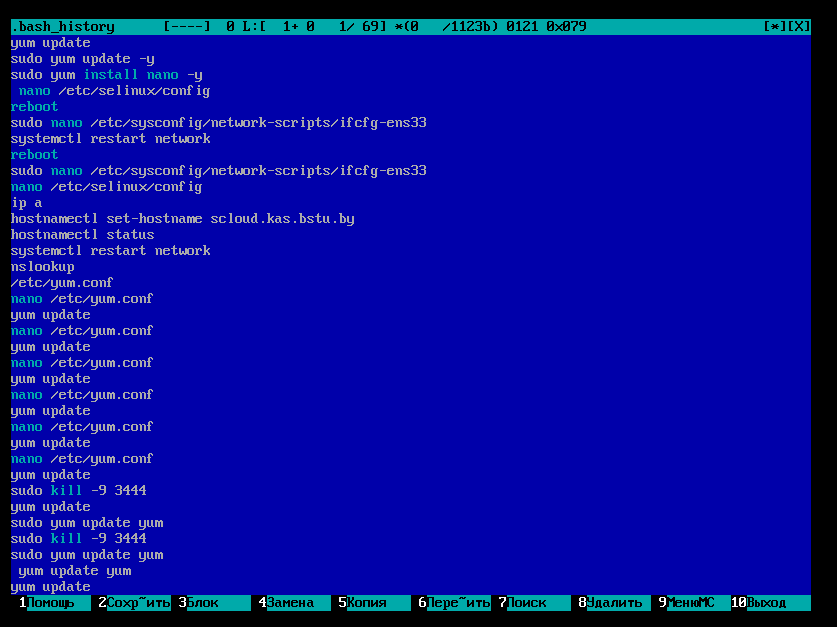
Удаление файлов или директорий можно осуществить при помощи нажатия **клавиши F8.**



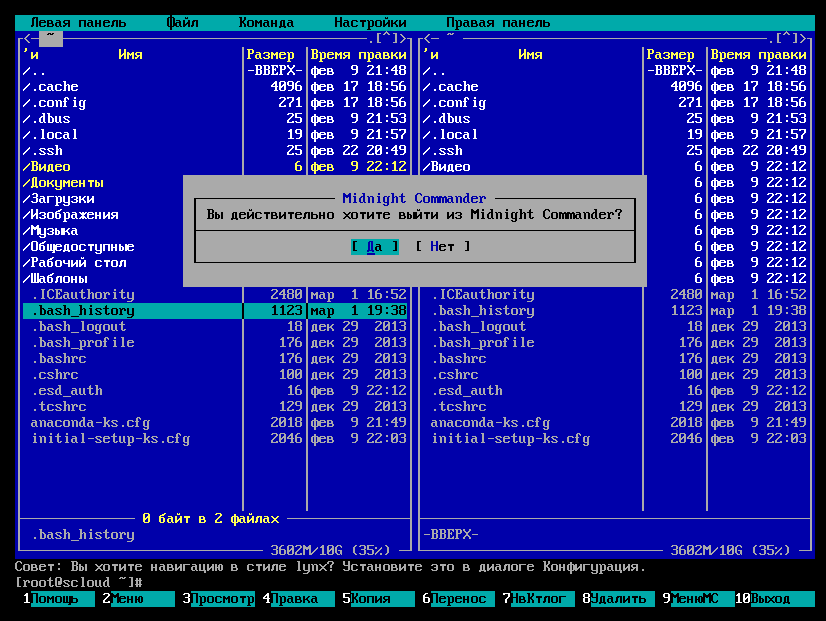
Для создания новых каталогов служит **клавиша F7**



Открытие файлов с возможностью изменения содержимого доступно в mc при помощи **клавиши F4**. **Выйти ESC**

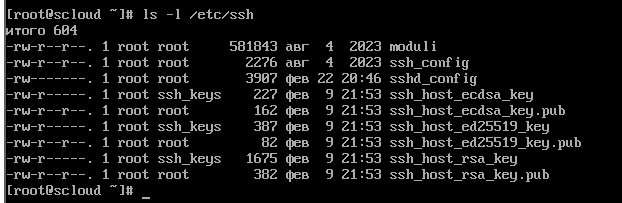


Выйти из оболочки можно при помощи **клавиши F10**

****

**Настройка службы SSH в операционной системе CentOS 7**

Для того, чтобы убедиться, что на машине виртуального узла установлен сервер SSH, необходимо просмотреть содержимое папки /etc/ssh. Если есть файл ssh-config, значит сервер SSH установлен.



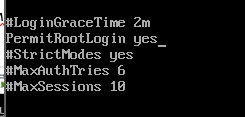
Для настройки сервера SSHd, который будет прослушивать по умолчанию 22 порт и который будет позволять пользователям устанавливать шифрованное соединение, аутентифицироваться и выполнять команды на удаленной системе, необходимо открыть файл редакторе nano

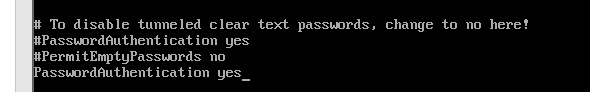
**# nano /etc/ssh/sshd\_config**

Раскоменчиваем строки

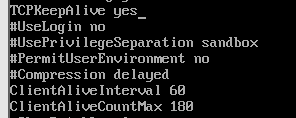
PermitRootLogin yes

PasswordAuthentication yes





1. Во всех ОС в целях безопасности устанавливается тайм-аут неактивной работы пользователя, по истечение которого интерфейс пользователя блокируется и ему предлагается пройти аутентификацию для продолжения работы. **Для изменения этого времени настроим тайм-аут при работе с использованием SSH надо Найти, раскомментировать и изменить следующие строки**

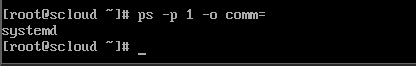


На машине виртуального узла в файле /etc/ssh/sshd\_config производятся те же действия.

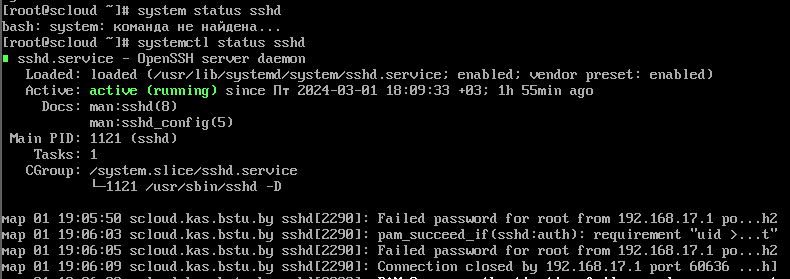
Теперь, сессия SSH не будет быстро разрываться, пока вы думаете

**Разрешить автоматический запуск сервера службы SSH при старте системы**

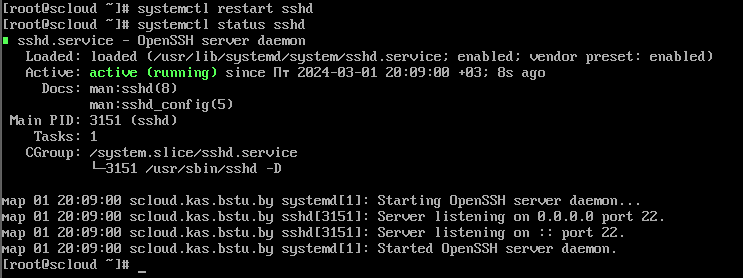
Сперва убедимся, что операционная система действительно использует systemd



Проверка запущена ли служба сервера SSHD (**active running**)



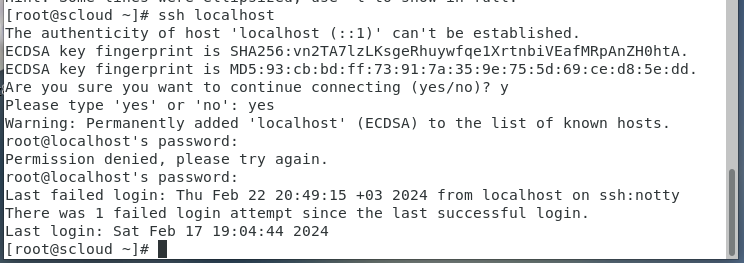
Для того, чтобы изменения в конфигурации вступили в силу, нужно вызвать команду **systemctl restart sshd**



Проверить работу служб SSHD на обоих узлах.

На управляющем выполнить подключение к самому себе:

# ssh localhost



Должен произойти обмен ключами безопасности, потом должен быть запущен процесс проверки пароля, и если все будет правильно выполнено, то откроется сессия SSH.

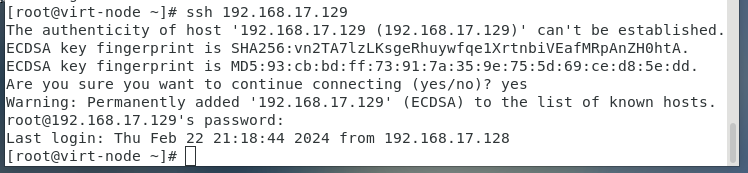
Для выхода из сессии SSH надо ввести:

# exit

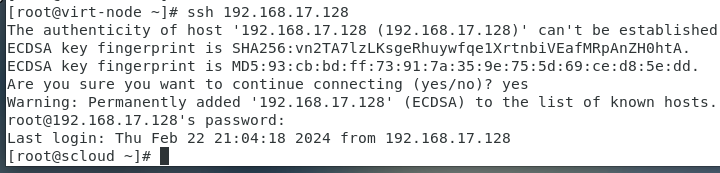


Подключение узлов друг к другу

С узла scloud



С узла virt-node



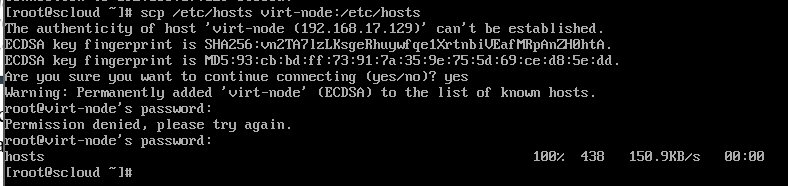
Если эти подключения выполняются без ошибок, то это означает, что на обоих узлах службы SSHD (сервер ssh) настроены и работают правильно.

**Копирование файла /etc/hosts на рабочий узел и хозяйскую машину**

На машине scloud выполнить команду:

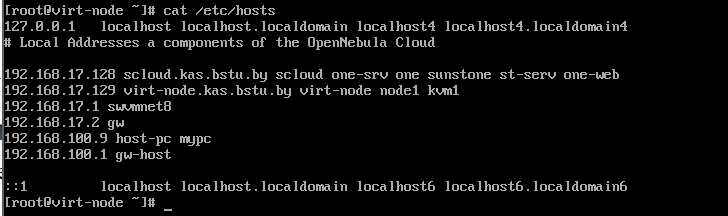
**scp /etc/hosts virt-node:/etc/hosts**

SCP позволяет передавать файлы между разными машинами в сети. Он использует ту же безопасную шифрованную связь, которую предоставляет SSH, для защиты передаваемых данных от несанкционированного доступа в момент передачи.



Проверим правильность выполнения, для чего на узле virt-node смотрим содержимое файла /etc/hosts:

**# cat /etc/hosts**



Теперь и на узле virt-node можно использовать имена вместо IP адресов.

**Копирование файла /etc/hosts на хозяйскую машину**

Копирование файла /etc/hosts с узла scloud на хозяйскую машину можно выполнить несколькими способами:

- отредактировать этот файл на хозяйской машине вручную (c:\Windows\System32\drivers\etc\hosts);

- скопировать из терминала Linux в ручную;

- с помощью программы WinSCP.

WinSCP – это программа для Windows, которая предоставляет графический интерфейс пользователя для использования протокола SCP (Secure Copy), а также протоколов SFTP (SSH File Transfer Protocol) и FTP (File Transfer Protocol). Это удобный способ передачи файлов между локальной машиной и удаленным узлом с гарантией безопасного соединения SSH.

**Копирование файла при помощи WinSCP:**

1. необходимо указать параметры ssh соединения которое будет установлено между хозяйской машиной и узлом scloud и которое будет использоваться для копирования файлов между машинами. Такими параметрами являются:

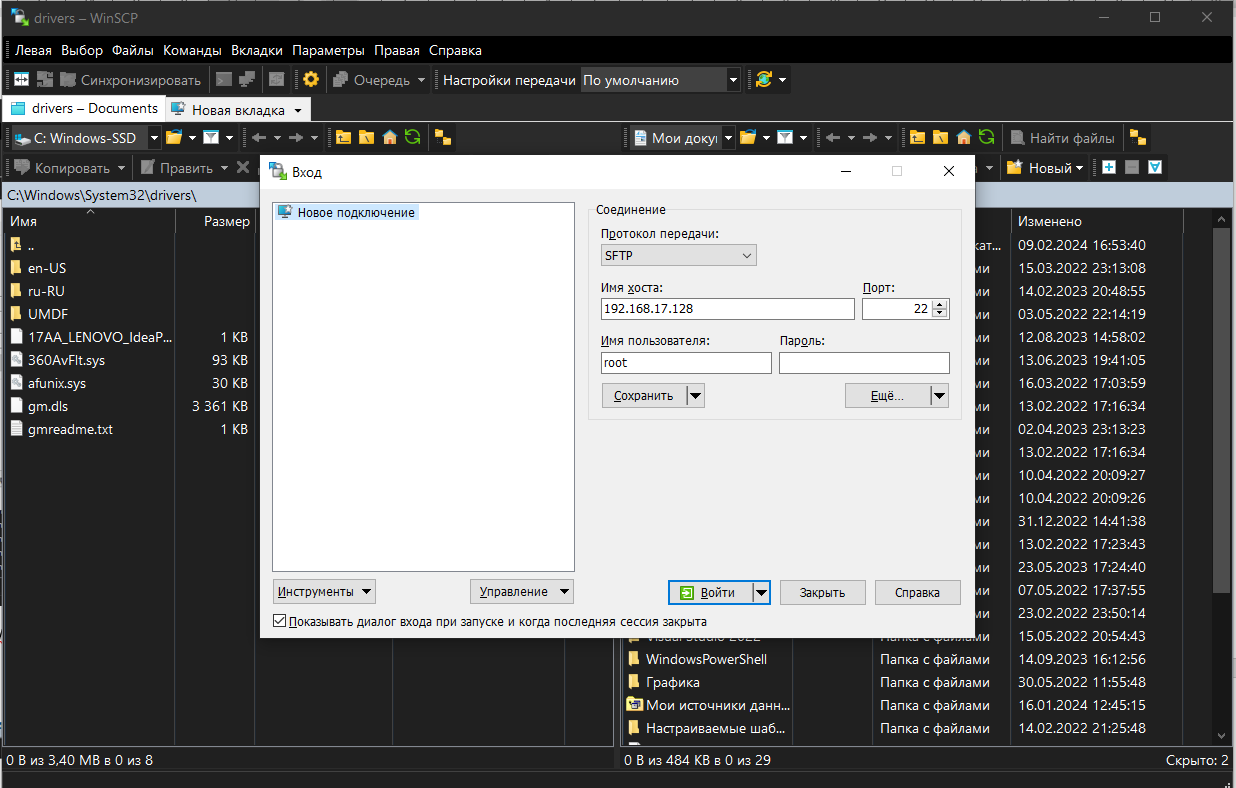
- протокол передачи: из выпадающего списка выбрать SCP

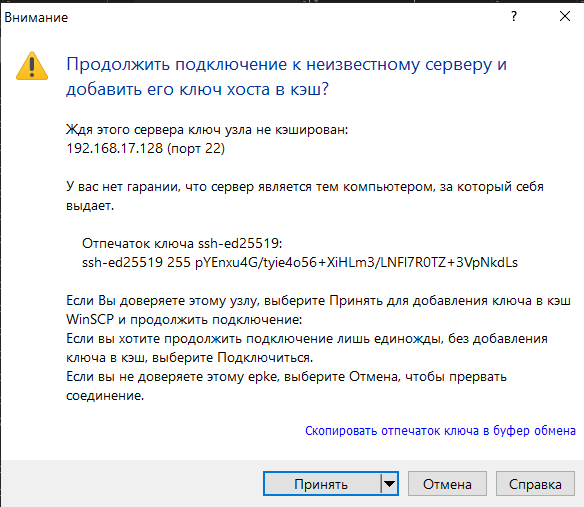
- имя хоста: 192.168.17.129

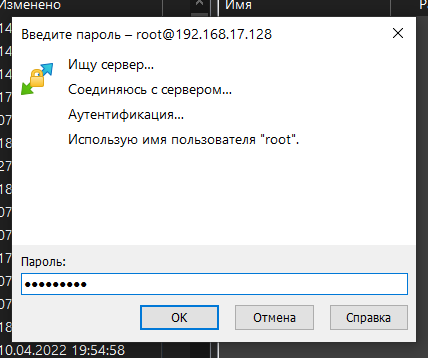
- порт: 22 (ssh);

- имя пользователя: root

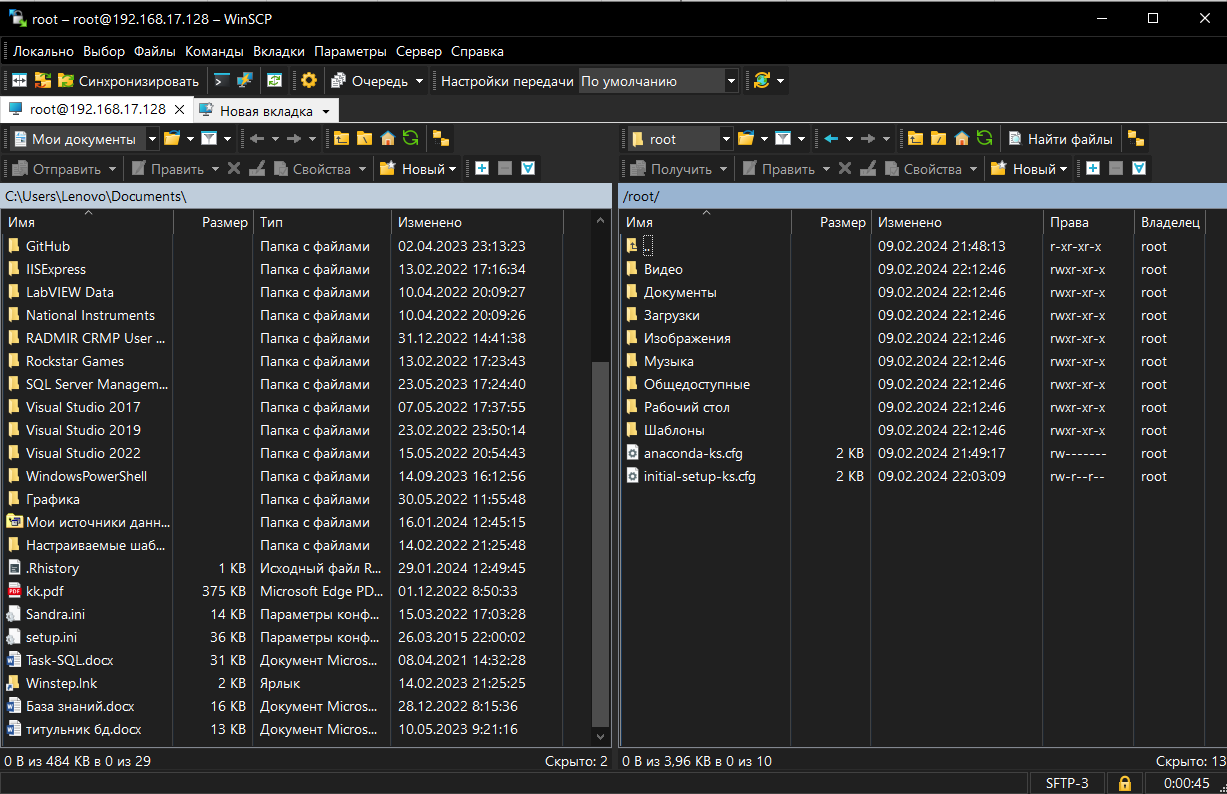
- пароль: оставить пустым.



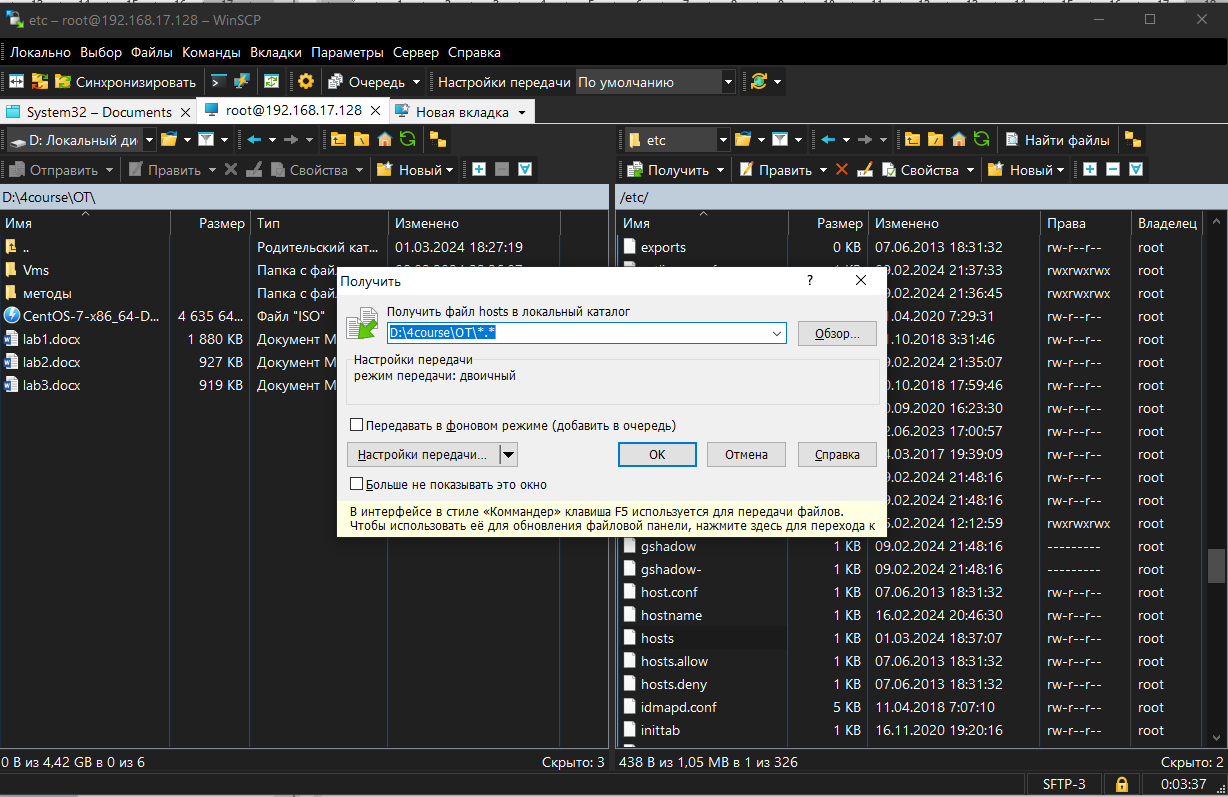


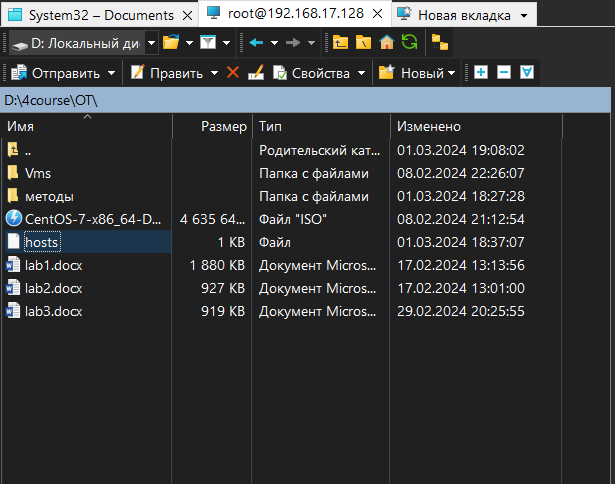


Если аутентификация на сервере scloud будет пройдена успешно, то откроется основное окно WinSCP имеющее вид схожий с TotalComander.

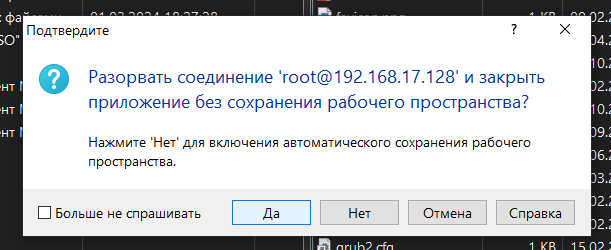


При помощи клавиши **F5** можно скопировать файл с удаленного узла на хостовую машину.

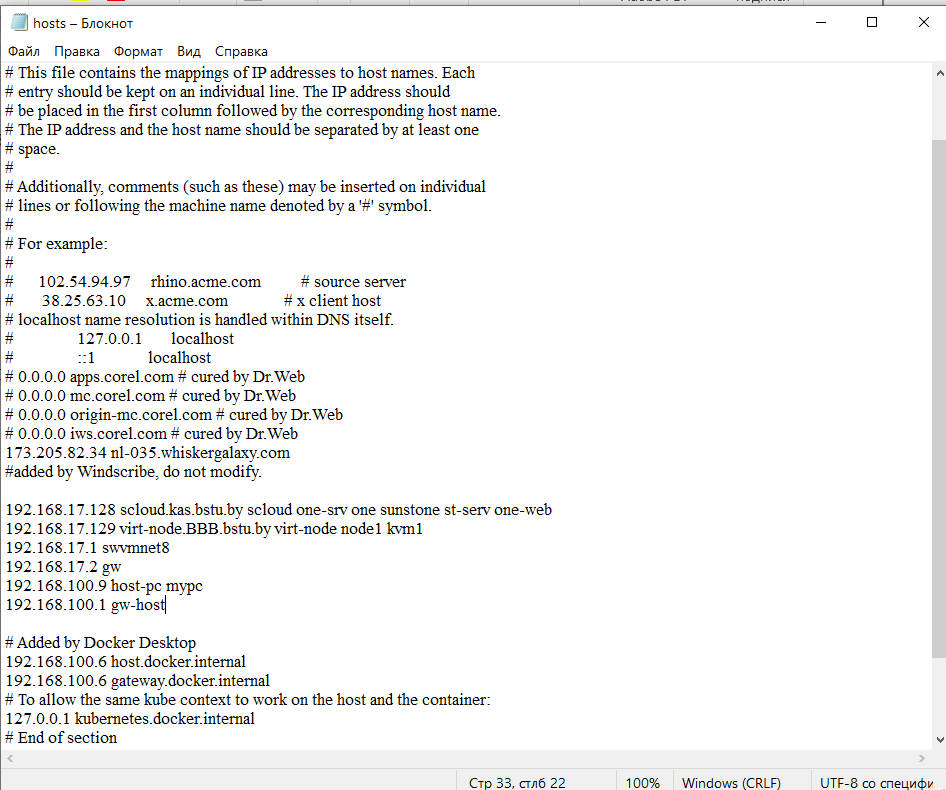


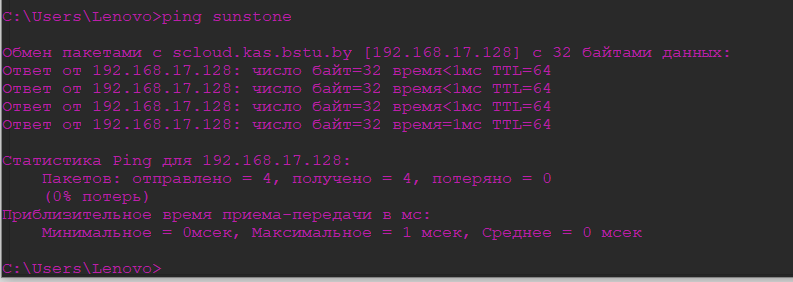


Подтверждение закрытия соединения



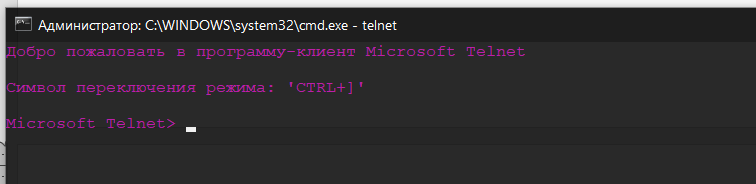
Проверить правильность настройки локальных имен в файле hosts можно при помощи команды **ping** к центральному узлу из хозяйской машины



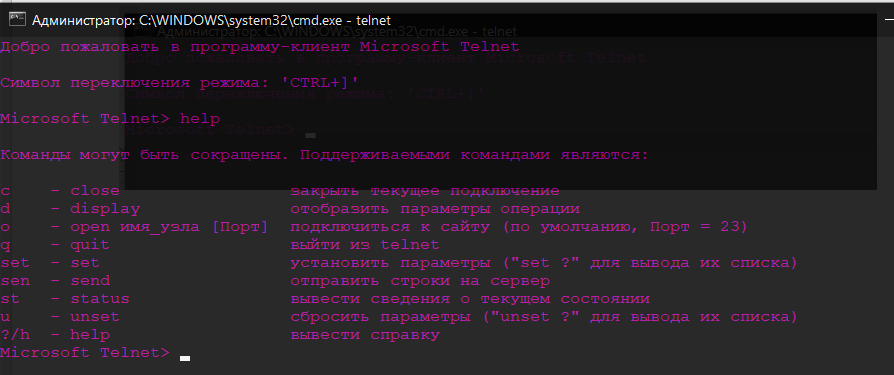


**Telnet**

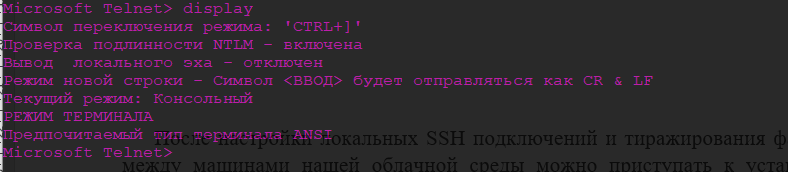
Для того чтобы запустить клиент Telnet, необходимо в командной строке прописать **telnet**



С помощью команды help можно получить справку по доступным командам



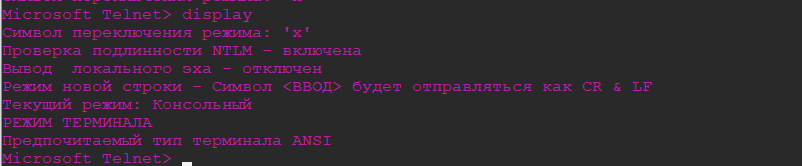
Просмотреть рабочие параметры с помощью команды **display**



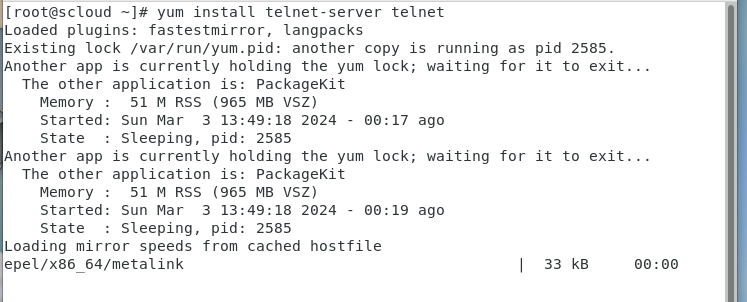
Изменить значение комбинации символов, используемое для переключения между командным и терминальным режимами работы, можно используя команду: **Microsoft Telnet>set escape x (x-**новая комбинация клавиш CTRL+3**)**

****

Проверяем при помощи команды **display**

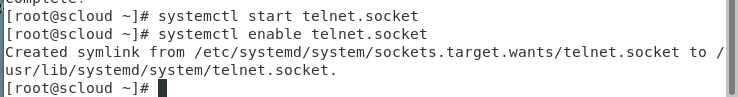


Устанавливаем telnet на управляющий узел

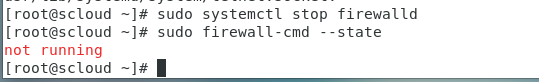


Необходимо запустить службу при помощи команды **systemctl start telnet.socket**

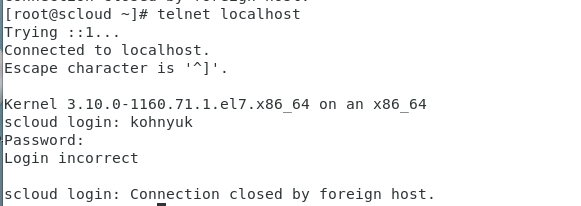
И переводим в автозапуск



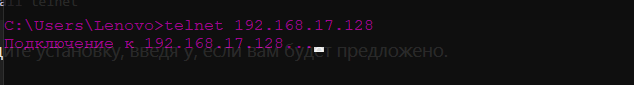
Для того чтобы беспрепятственно принимать подключения на **23 порту** (порт, который по умолчанию используется службой Telnet), рекомендуется отключить firewall на машине виртуального узла при помощи команды **sudo systemctl stop firewalld**

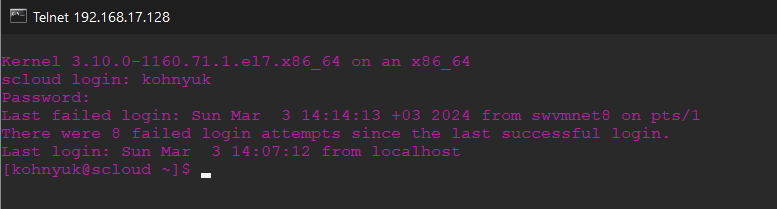


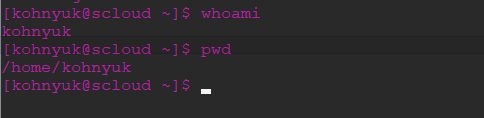
Проверка доступности службы (подключения к хосту текущей машины)



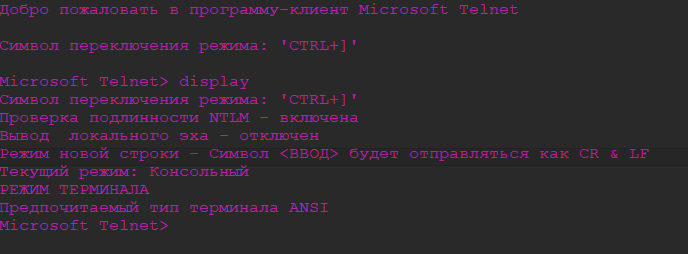
Подключаемся к управляющему узлу



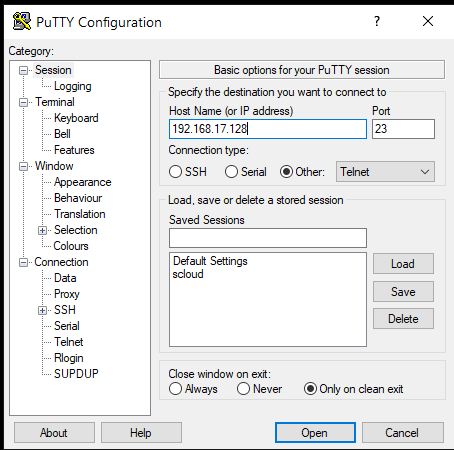


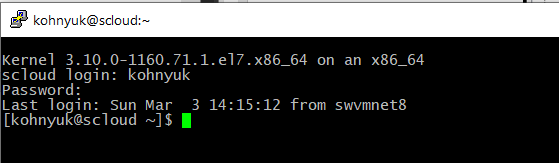


Далее необходимо восстановить символ переключения режима на предыдущий.

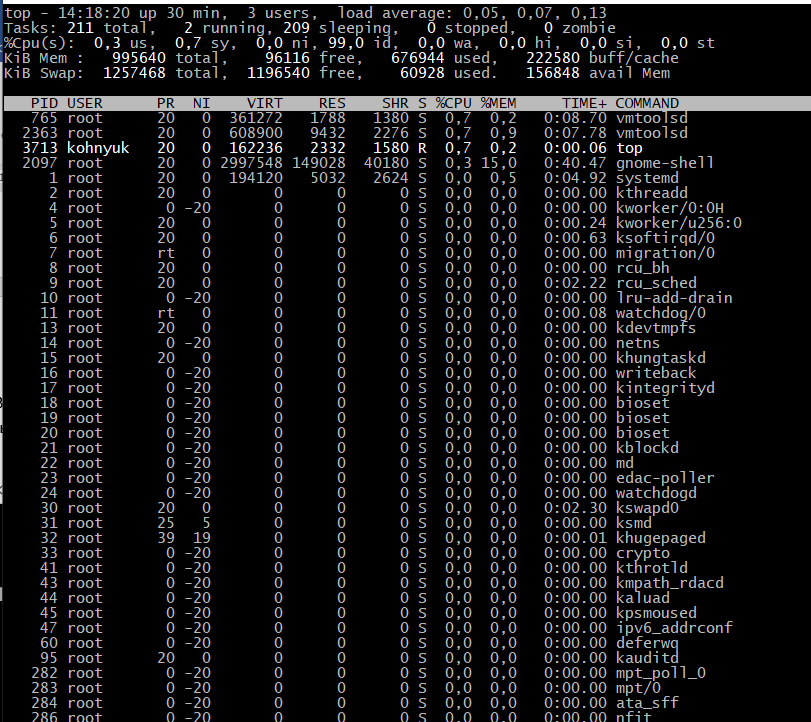


**Использование программы PuTTY в качестве клиента Telnet**





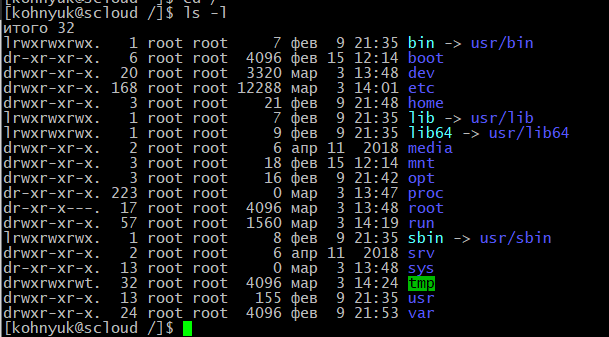
Команда **top -** команда просмотра загрузки сервера, выход из top: – q



$cd / команда перехода в корневой каталог



$ls –l просмотр содержимого текущего каталога



$pwd выводит имя текущего каталога



$cd /home/…./ переход в каталог. Переходим в каталог, имя которого совпадает с именем текущего пользователя



Создаем файл 1.txt с помощью команды:

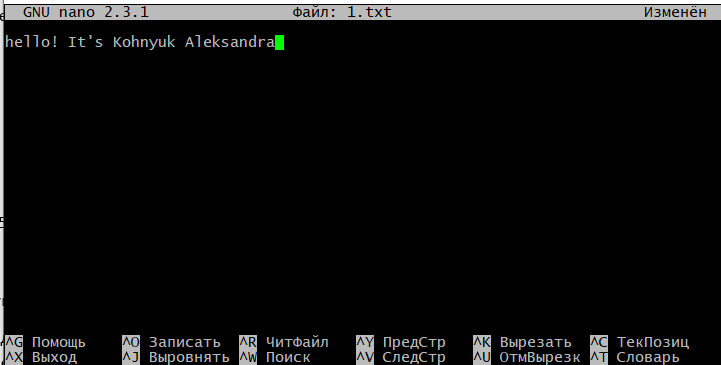
**$touch 1.txt**

****

Открываем этот файл на редактирование:

**$nano 1.txt**

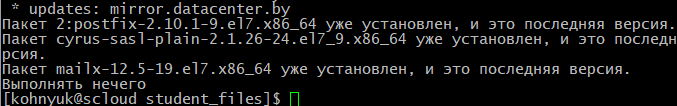
В файл следует ввести текстовую строку для ее дальнейшей отправки по электронной почте.

****

Для того, чтобыотправить письмо при помощи электронной почты, необходимо установить пакеты **Posrfix, cyrus-sasl-plain и mailx**

* **Postfix** представляет собой почтовый сервер
* **cyrus-sasl-plain** – пакеты механизмов его аутентификации
* **mailx** — утилита командной строки для отправки почты

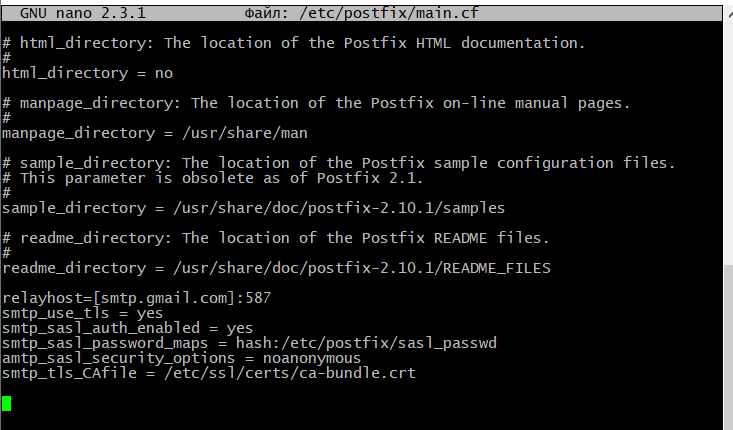
**sudo yum install -y postfix cyrus-sasl-plain mailx**

****

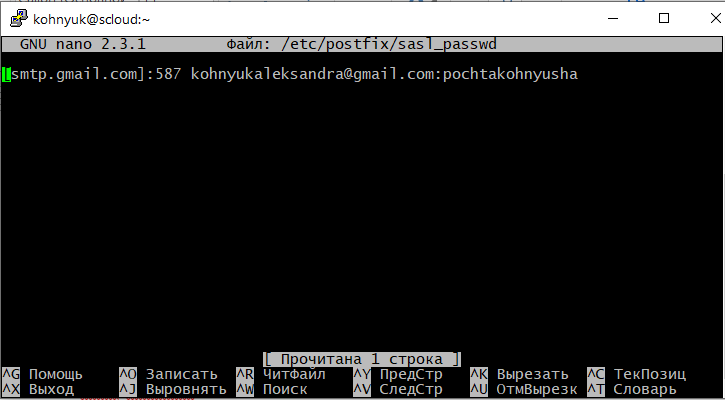
После установки необходимо произвести конфигурацию почтового сервера и внести изменения в файл **/etc/postfix/main.cf.**

В конце файла требуется прописать установку значений для параметров

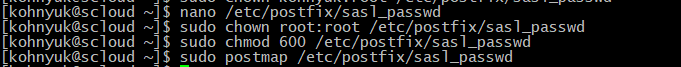
* **relayhost**
* **smtp\_use\_tls**
* **smtp\_sasl\_auth\_enabled**
* **smtp\_sasl\_password\_maps**
* **amtp\_sasl\_security\_options**
* **smtp\_tls\_CAfile**

****

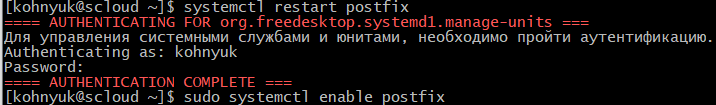
В **файл /etc/postfix/sasl\_passwd** необходимо записать учетные данные электронной почты.

****

После занесения информации о паролях, необходимых для аутентификации при работе с Postfix, следует вызвать команды для изменения владельца и группы владельца указанного файла на пользователя root, для изменения прав доступа и для создания базы данных почтового сервера Postfix из файла конфигурации /etc/postfix/sasl\_passwd

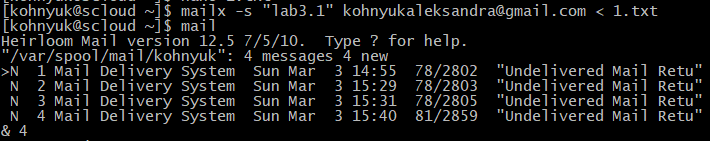
****

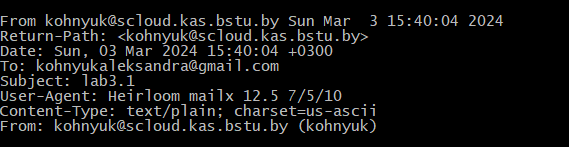
После внесенных изменений в конфигурацию Postfix рекомендуется перезапустить службу почтового сервера и активировать ее

****

Отправка письма

Команда **mail** - будет выдан список поступивших сообщений

****

****

После настройки локальных SSH подключений и тиражирования файла hosts между машинами нашей облачной среды можно приступать к установке ПО OpenNebula.