**Облачные технологии**

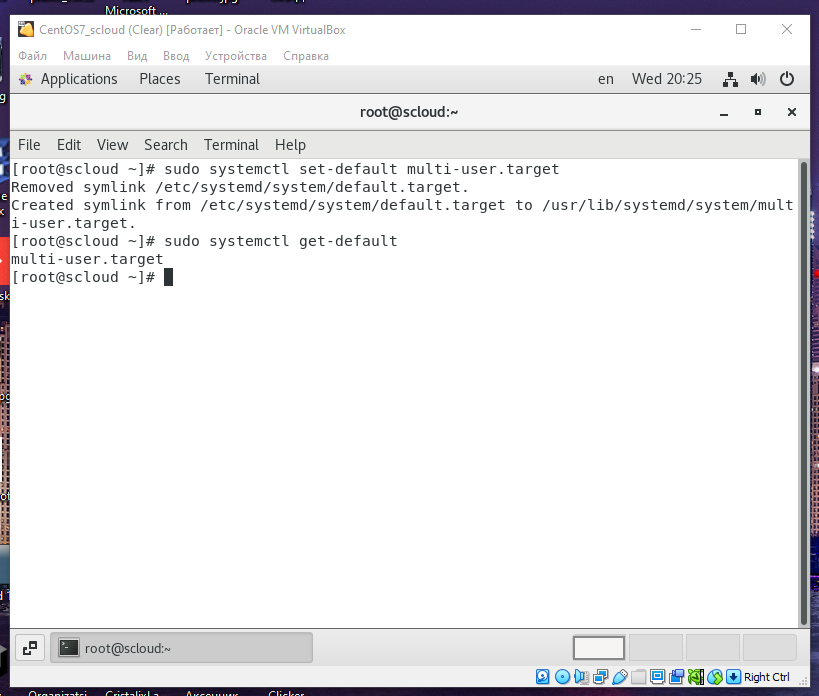
Лабораторная работа № 3

**Подготовка виртуальных машин к развертыванию облака OpenNebula**

**1. Подготовка виртуальных машин к развертыванию облака OpenNebula**

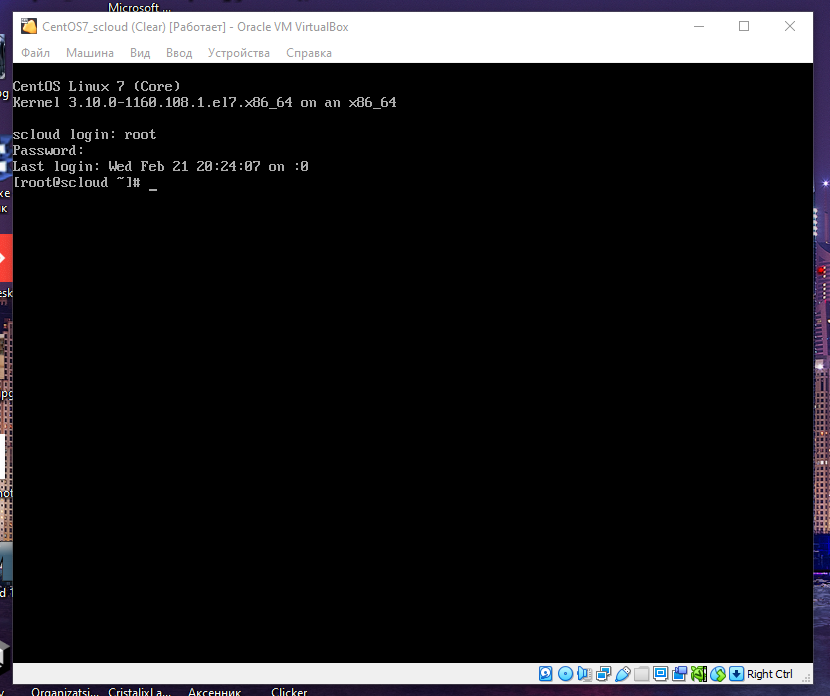
**1.1. Отключение GUI (X-Windows) при загрузке CentOS**

Отключить запуск X-ов при старте системы можно выполнив команду:



Перезагружаемся без GUI

$ sudo reboot



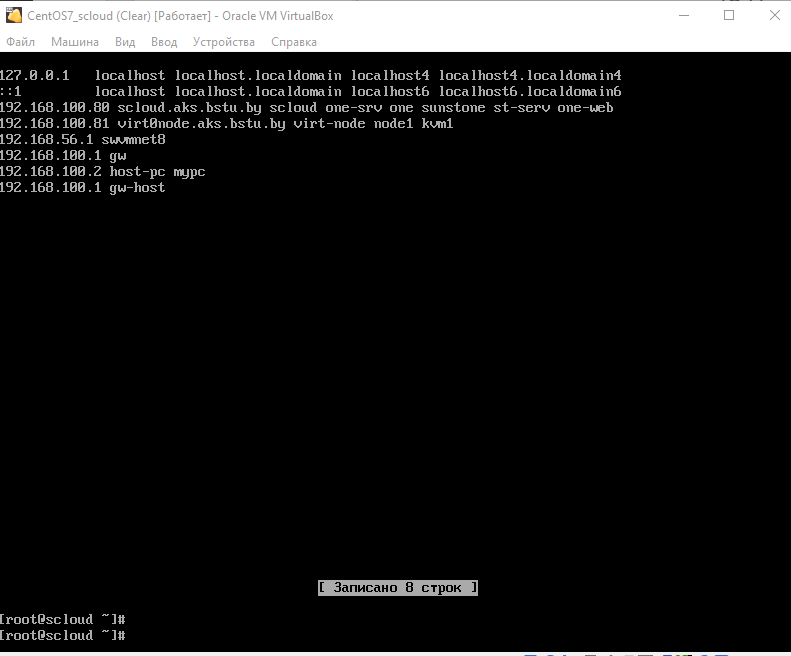
**1.3 Настройка преобразования имен в IP адреса в ОС Linux.**

Заполните таблицу имен и IP адресов ВМ входящих в состав облака:

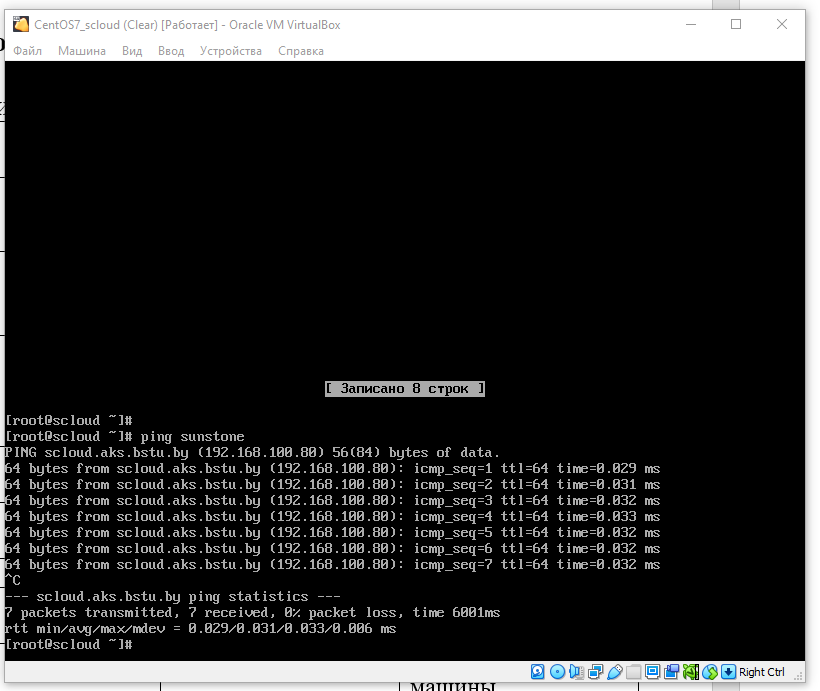
|  |  |  |  |
| --- | --- | --- | --- |
| № п.п | Имя узла\* | IP адрес узла\*\* | Назначение узла |
| 1 | **Scloud.aks.bstu.by**  one-serv | 192.168.100.80 | Сервер OpenNebula |
| 2 | **sunstone**  st-serv  one-web | 192.168.100.80 | Web-сервер Sunstone управления облаком |
| 3 | **virt\_node**  virt-node1  node1  kvm1 | 192.168.100.81 | Сервер виртуализации |
| 4 | **swvmnet8** | 192.168.56.1 | Виртуальный коммутатор VmNet8 |
| 5 | **gw** | 192.168.100.1 | Шлюз виртуальной сети облака |
| 6 | dns-srv | 192.168.100.1 | Сервер DNS |
| 7 | host-pc  mypc | 192.168.100.2 | Хозяйская машина |
| 8 | **gw-host** | 192.168.100.1 | Шлюз хозяйской машины |

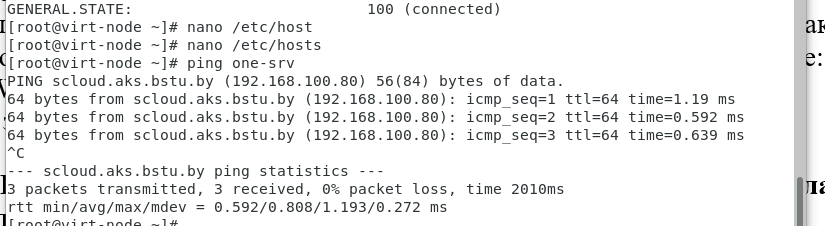
**1.3.1 Внесение имен узлов облака в файл /etc/hosts на управляющем узле**

На управляющем узле scloud откроем файл /etc/hosts:

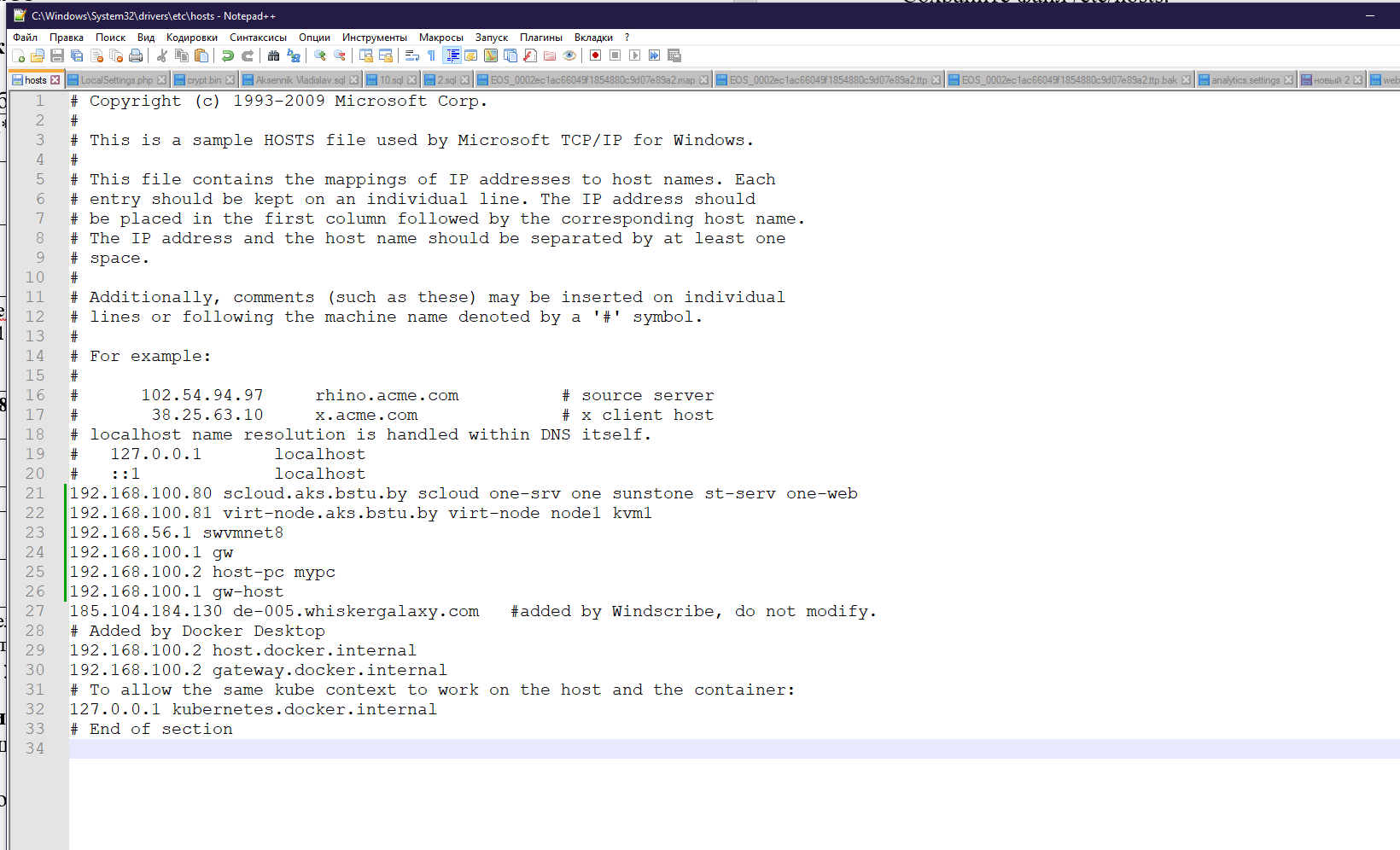


Проверить правильность назначения имен можно с помощью команды ping:

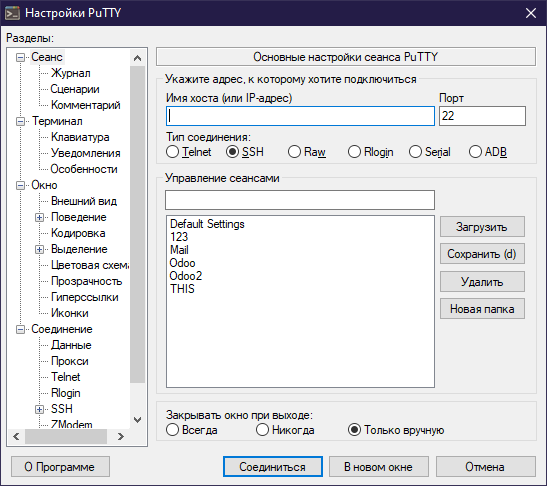




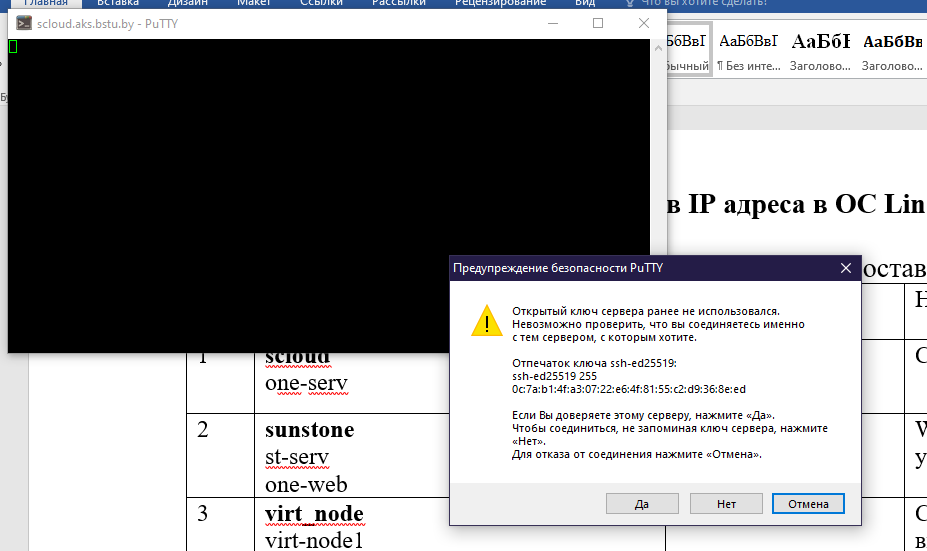
- c:\Windows\Ststem32\drivers\etc\hosts



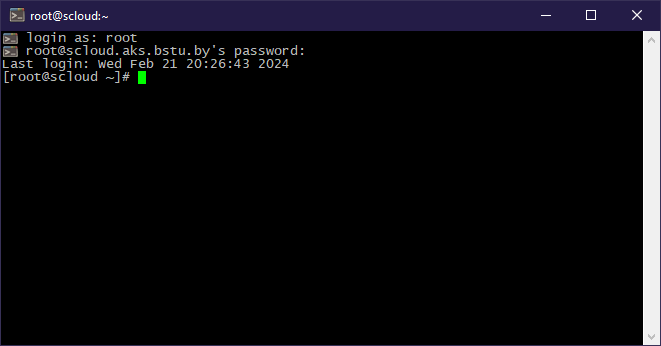
**Знакомство со средствами удаленного администрирования узлов сетевой инфраструктуры облаков.**

. Работа со службой SSH. 

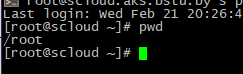
Настройте программу PuTTY на работы по протоколу SSH. Подключитесь к учебному серверу по протоколу SSH, нажав кнопку "Open" в окне программы PuTTY. Появиться окно, сообщающее о том, что для данного сервера в реестре отсутствуют ключи шифрования.



.2 Выполните аутентификацию на учебном сервере, для чего в появившемся окне терминала в строке приглашения введите имя пользователя, а затем после появления соответствующей строки запроса введите пароль.

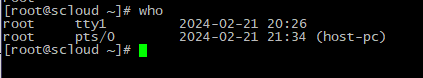


Войдя в систему, выполните команды:

$pwd – выводит имя текущего каталога; 

$whoami – выводит имя пользователя, под которым Вы вошли в систему; 

$who – показывает имена всех пользователей, находящихся в системе;

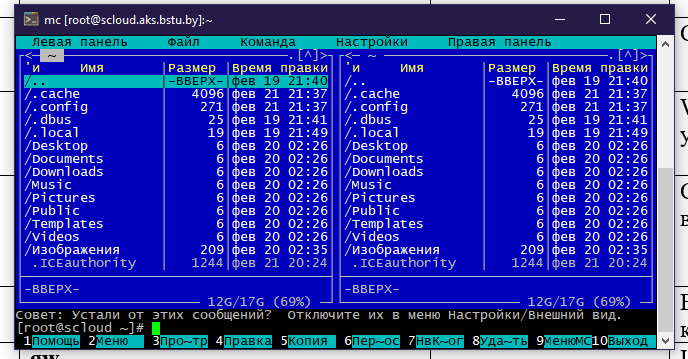


$deco – запускает командную оболочку, которая позволяет перемещаться по файловой системе и выполнять некоторые файловые команды, не зная команд ОС UNIX.



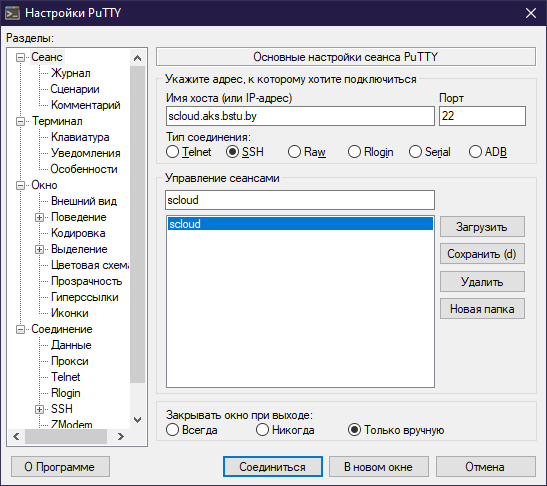
Эта программа во многом аналогична программе Norton Commander для ОС MS DOS.

Вызовите программу Midnight Commander с помощью одной из команд: $mc



**Рекомендации по настройке Putty**

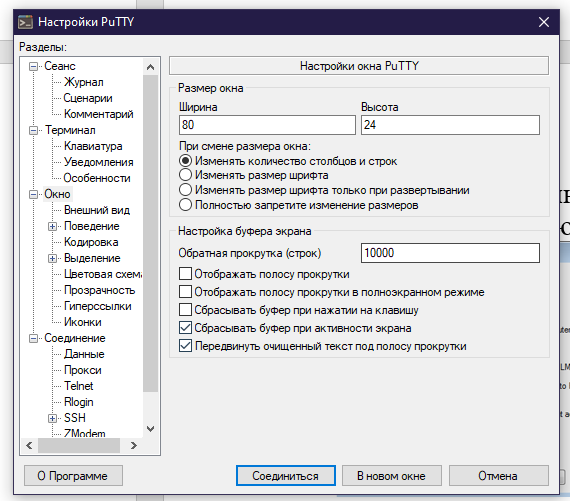
1) Всегда создавайте сохраненные сессии для работы с узлами требующими частых подключений:



Для этого служат кнопки Load и Save.

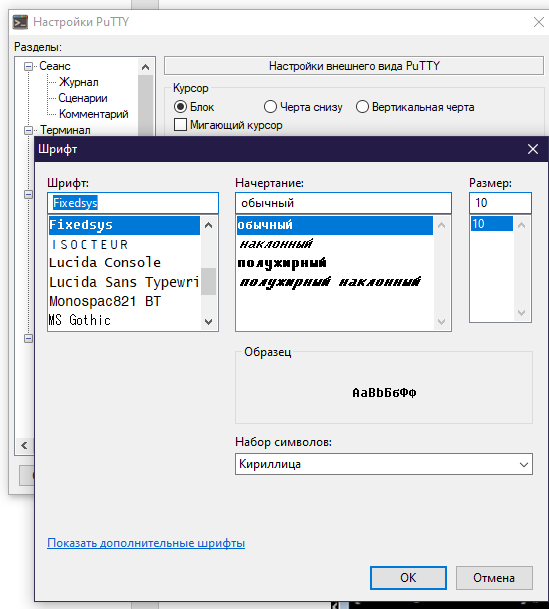
2) Настройки сессий для корректной работы с Midnight Commander:

**Window**

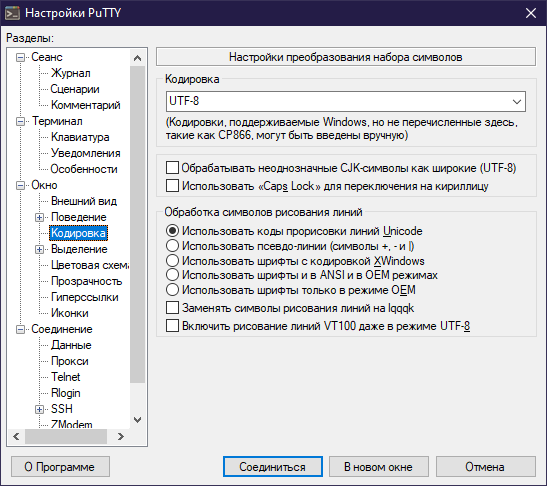


Установите размер буфера прокрутки экрана 20000 и более (макс. 32000)

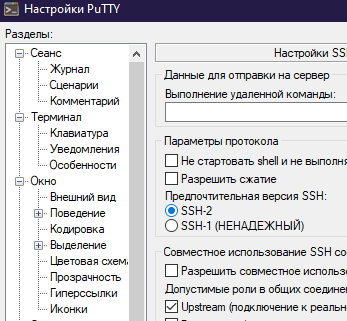
**Appearance**



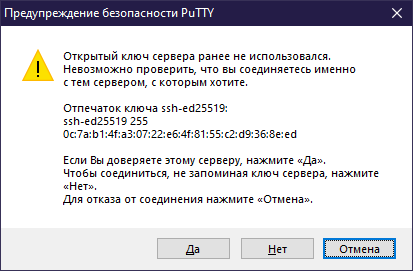
Установите шрифт Fixedsys 10-point, для чего кликните кнопку Change.



Выберите кодировку UTF-8

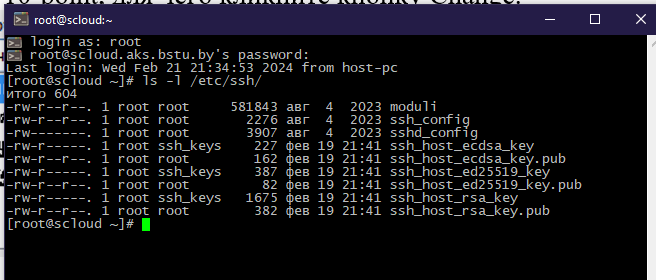


Выберите версию SSH 2

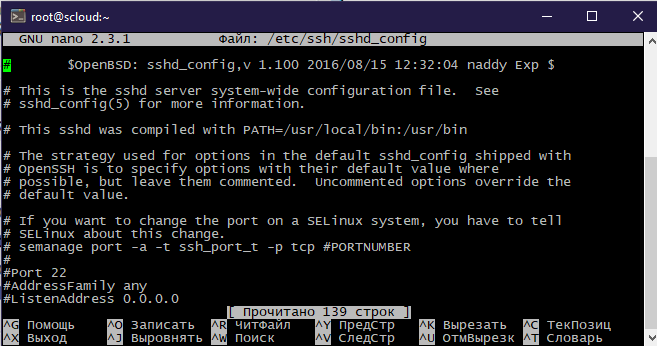


**1.4.2 Настройка службы сервер SSH в OS CentOS 7**

1) Просмотреть содержимое папки /etc/ssh:



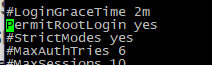
Для этого откройте файл в редакторе nano файл /etc/sshd\_config



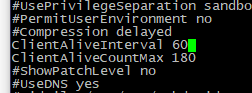
Раскомментируйте строки:

PermitRootLogin yes

PasswordAuthentication yes

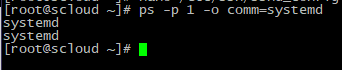
Во всех ОС в целях безопасности устанавливается тайм-аут неактивной работы пользователя, по истечение которого интерфейс пользователя блокируется и ему предлагается пройти аутентификацию для продолжения работы. Для изменения этого времени настроим тайм-аут при работе с использованием SSH надо Найти,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



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

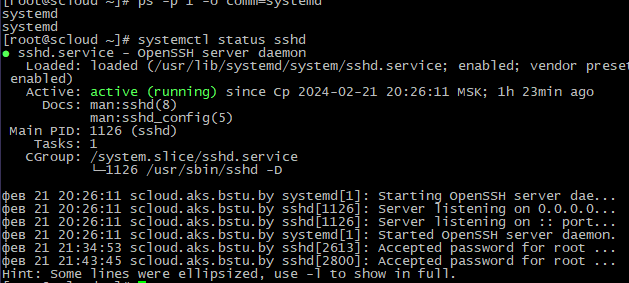
1) Сперва убедимся, что операционная система действительно использует systemd:

|  |
| --- |
| ps -p 1 -o comm= |

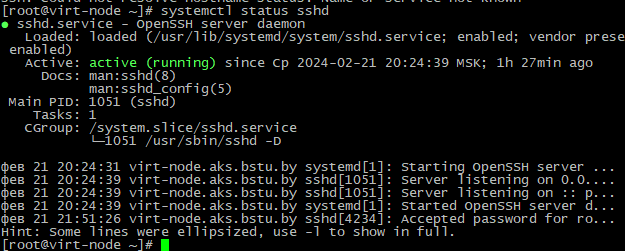


2) Проверим запущена ли служба сервера SSHD

# systemctl status sshd

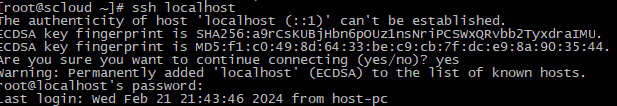


3) Проверить работу служб SSHD на обоих узлах:



На управляющем выполнить подключение к самому себе:

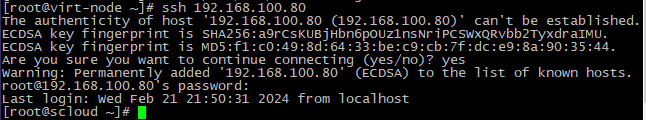
# ssh localhost



Если подключения к самому себе проходят, то надо проверить возможность подключения узлов друг другу в обоих направления.

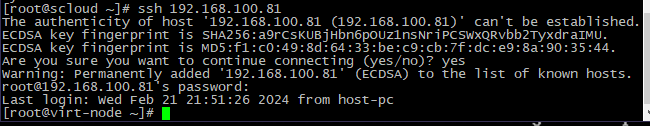
С узла virt-node:

# ssh 192.168.100.80



С узла scloud:

# ssh 192.168.100.81

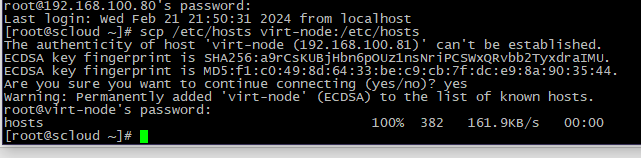


**1.4.3 Копирование файла /etc/hosts на рабочий узел и хозяйскую машину.**

Копирование на рабочий узел.

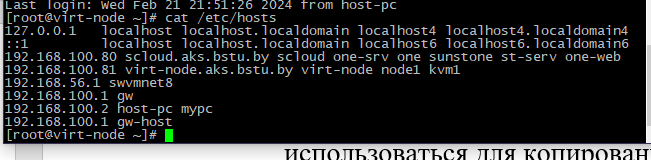
На машине scloud выполнить команду:

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



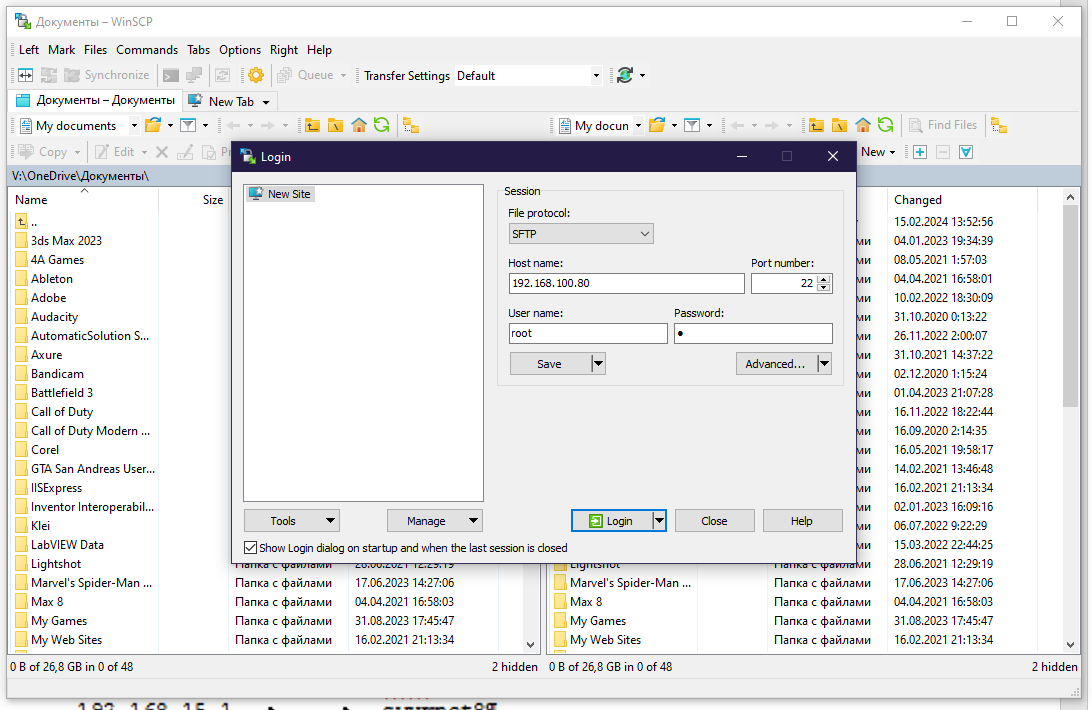
Проверим правильность выполнения, для чего на узле virt-node смотрим содержимое файла /etc/hosts:

# cat /etc/hosts

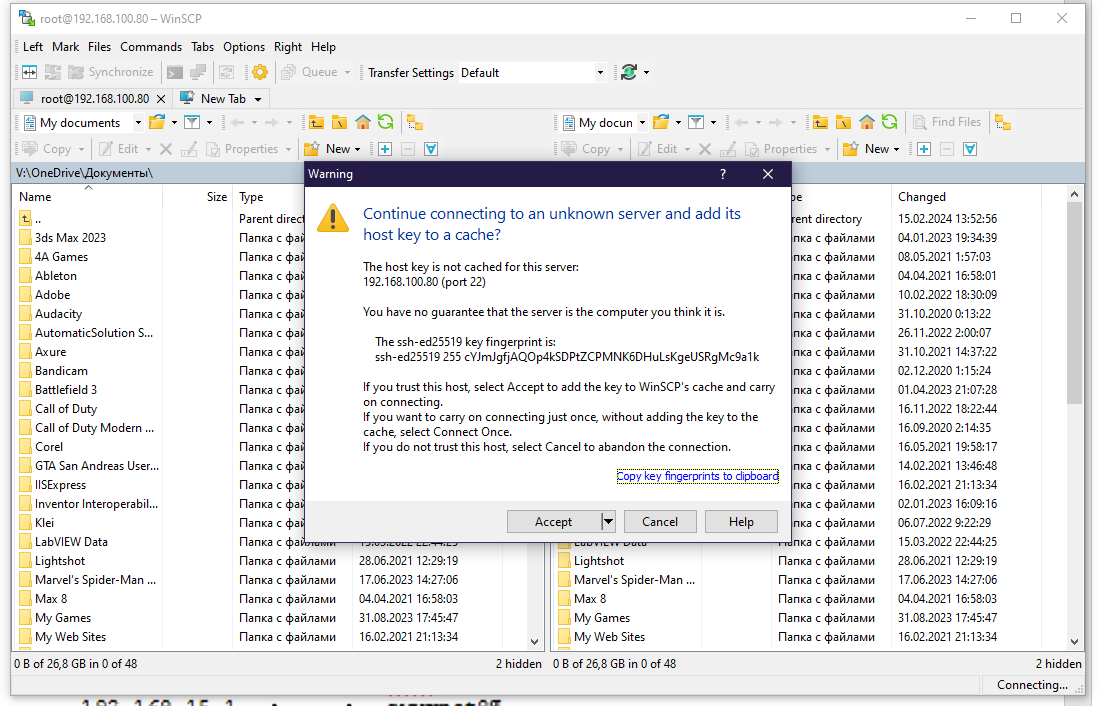


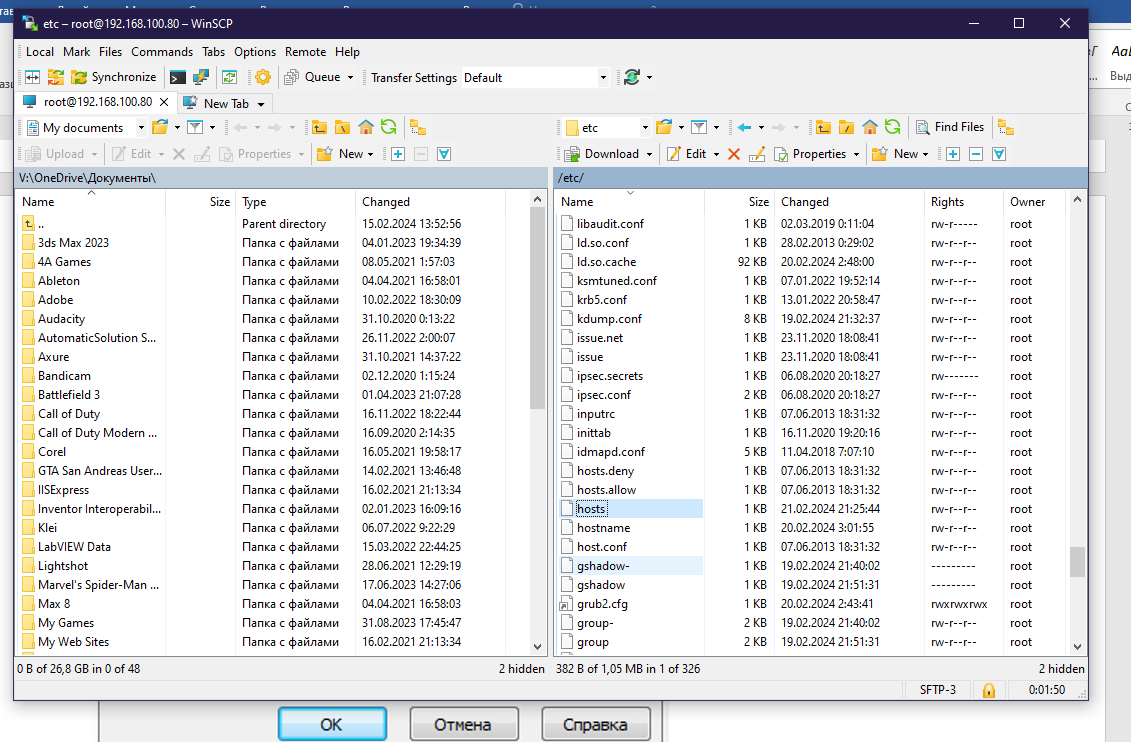
**Копирование файла /etc/hosts на хозяйскую машину**.

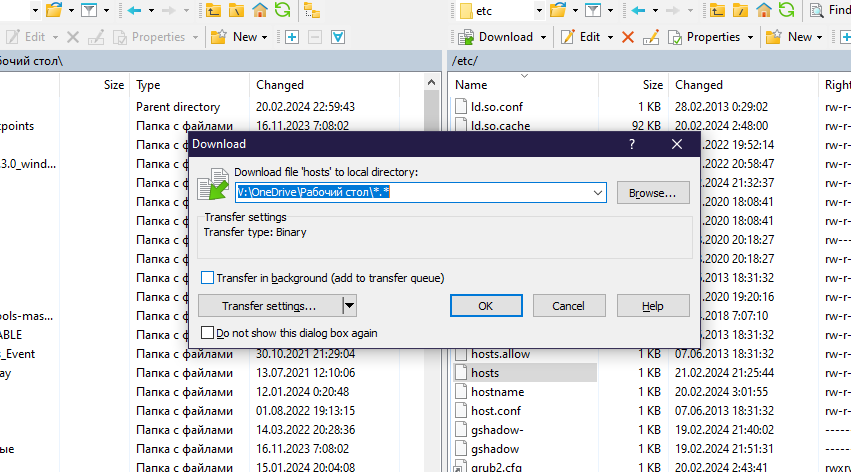
1) Ниже описан порядок копирования файла hosts с помощью WinSCP.



1. Откроется окно приема ключа.







te