**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:

$ sudo systemctl set-default multi-user.target

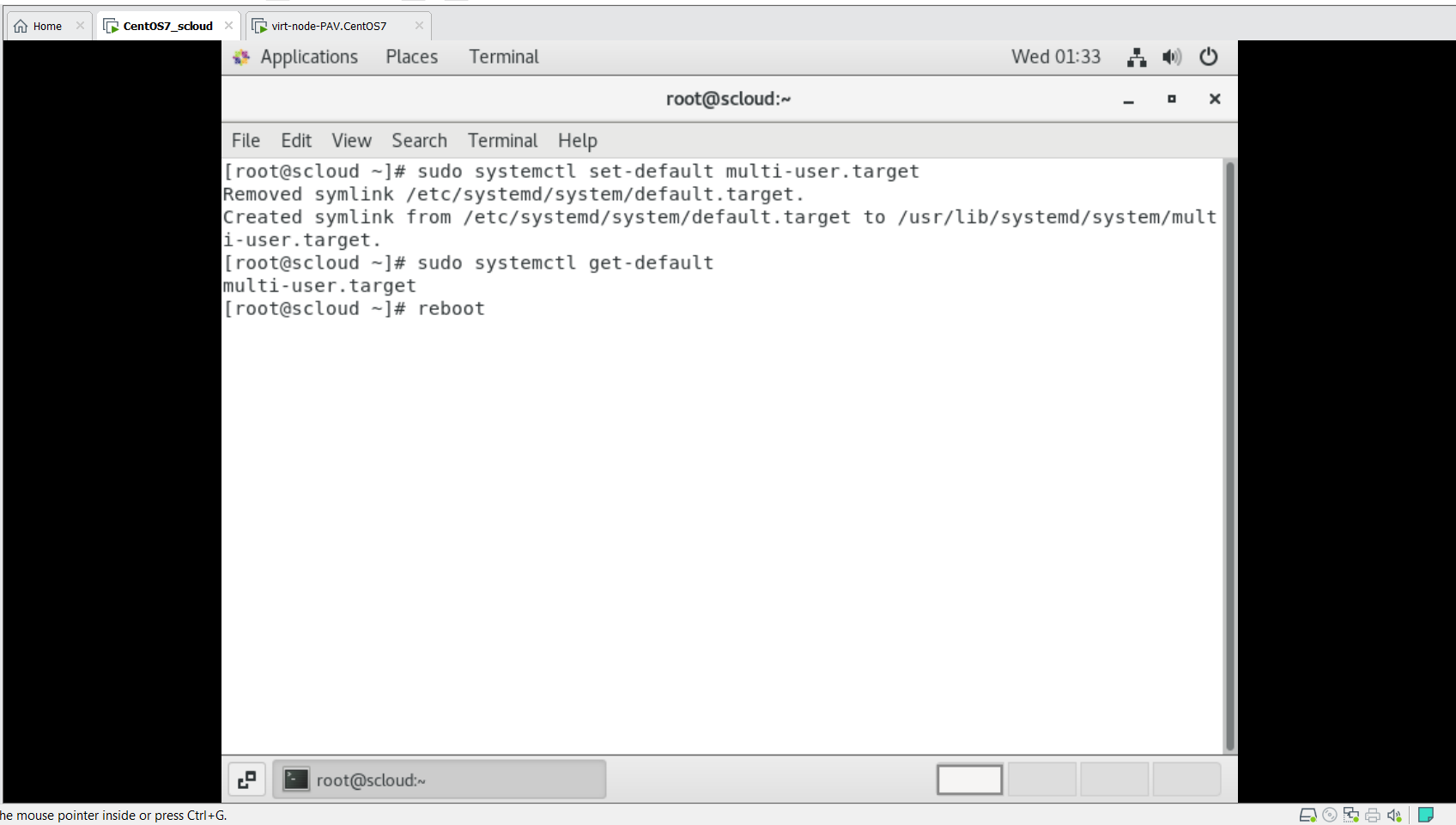
проверяем:

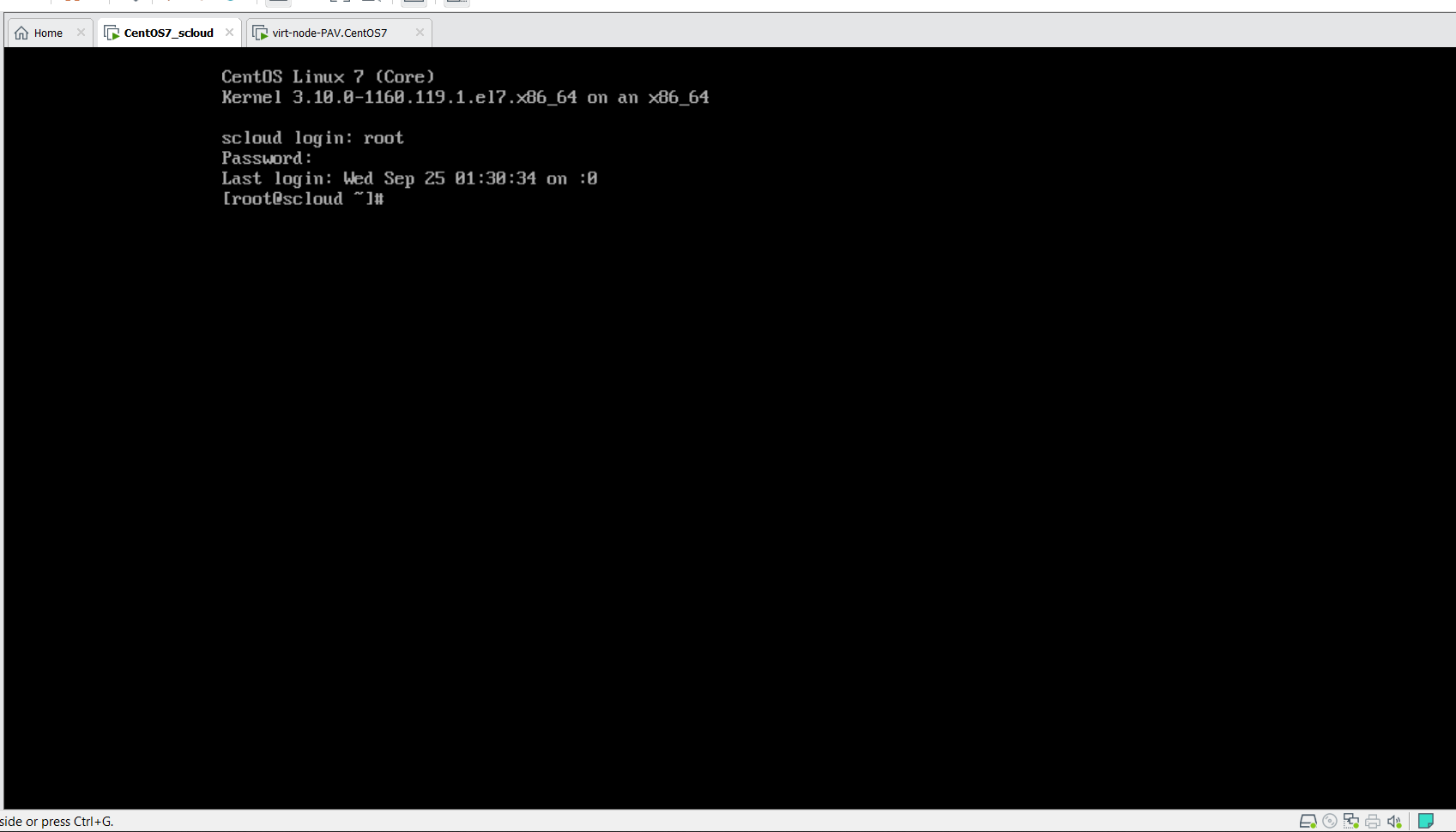
$ sudo systemctl get-default

$ multi-user.target

Перезагружаемся без GUI

$ sudo reboot





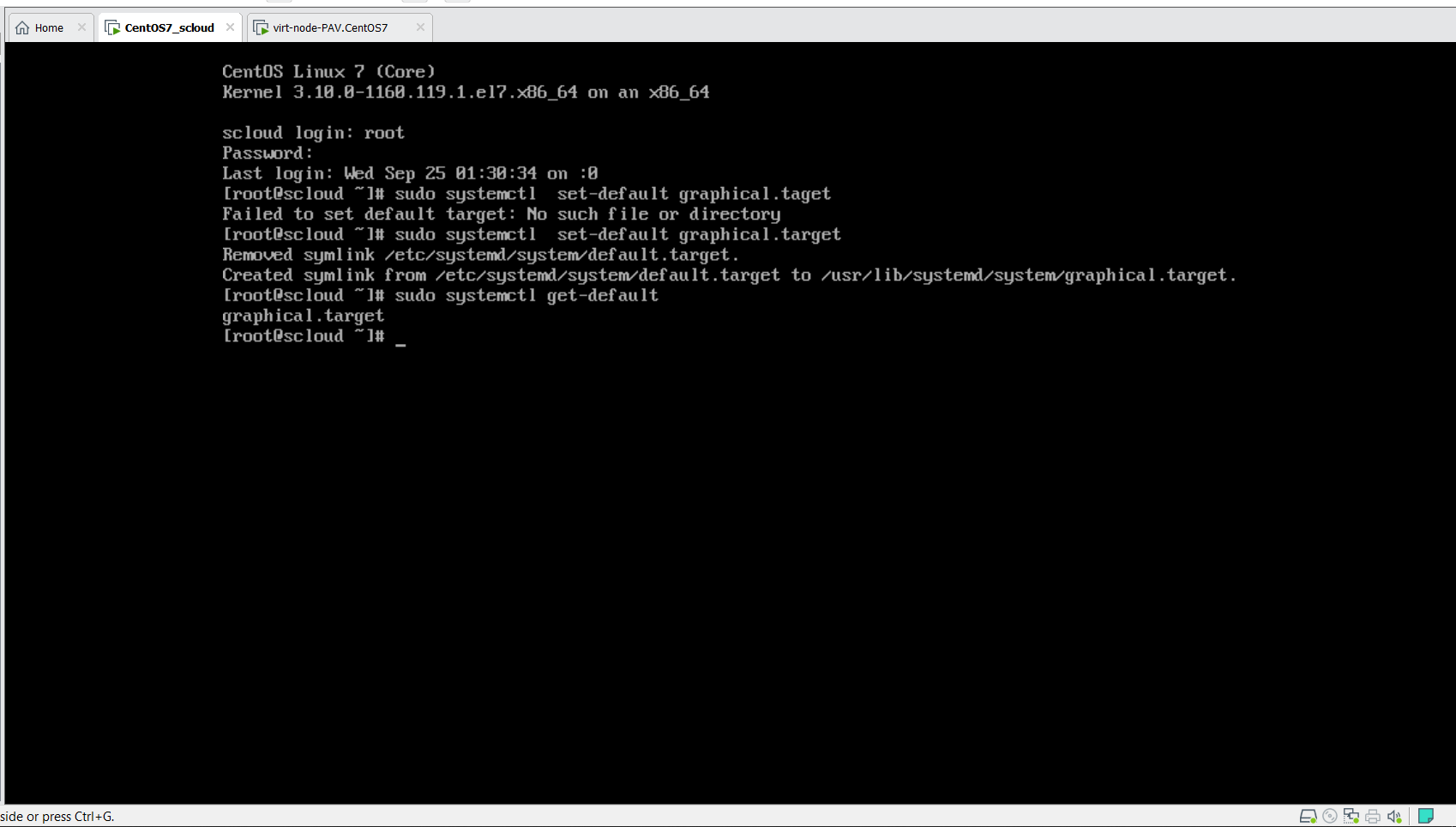
Вернуть обратно запуск графической оболочки можно с помощью команды:

$ sudo systemctl set-default graphical.target

проверяем:

$ sudo systemctl get-default

$ graphical.target



**1.2 Настройка виртуальных машин для работы через прокси**

Если при выполнении лабораторной работы вы работаете с использование сетевого подключения в компьютерном классе, в котором доступ машин к Интернет реализуется через прокси, то необходимо выполнить следующие настройки пользовательского окружения в ОС ВМ головного и рабочего хостов ОН (Орен Небула).

Замечание. Если Ваш доступ к Интернет не требует использования прокси-сервера, то п.1.2.1 выполнять не надо.

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

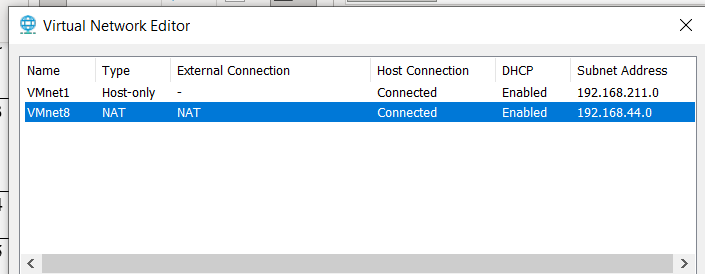
Заполните таблицу имен и IP адресов ВМ входящих в состав облака:

|  |  |  |  |
| --- | --- | --- | --- |
| № п.п | Имя узла\* | IP адрес узла\*\* | Назначение узла |
| 1 | **scloud**  one-serv | 192.168.44.130 | Сервер OpenNebula |
| 2 | **sunstone**  st-serv  one-web | 192.168.44.130 | Web-сервер Sunstone управления облаком |
| 3 | **virt\_node**  virt-node1  node1  kvm1 | 192.168.44.131 | Сервер виртуализации |
| 4 | **swvmnet8** | 192.168.44.1 | Виртуальный коммутатор VmNet8 |
| 5 | **gw** | 192.168.44.2 | Шлюз виртуальной сети облака |
| 6 | dns-srv | 192.168.44.2 | Сервер DNS |
| 7 | host-pc  mypc | 192.168.41.55 | Хозяйская машина |
| 8 | **gw-host** | 192.168.41.51 | Шлюз хозяйской машины |

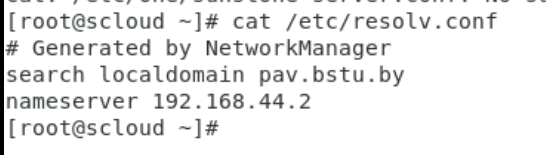
\* Жирным выделены имена ВМ присвоенные в качестве hostname, другие имена, приведенные в таблице, являются псевдонимами (алиасами).

\*\* Необходимо указать адреса определенные Вами в лаб.раб. 2

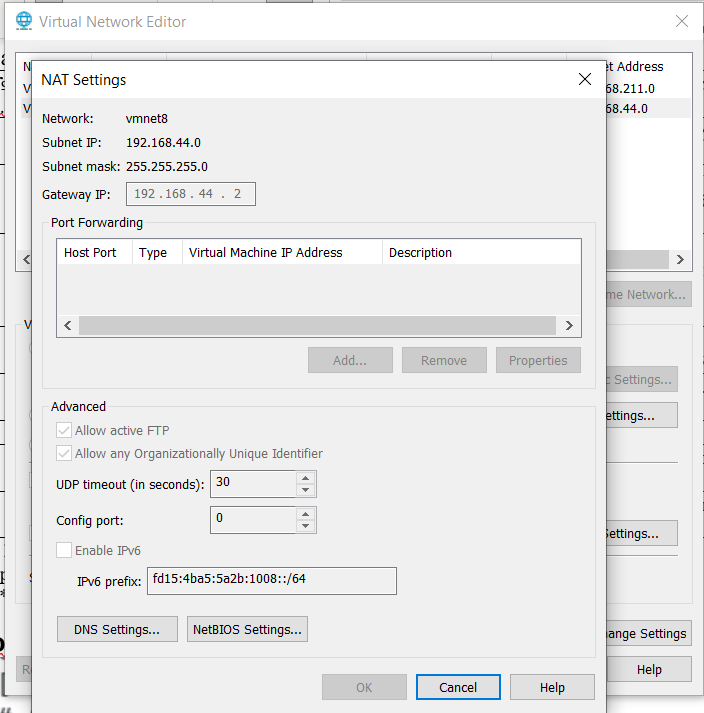
**Swvmnet8**



**Dns-sry**



**Gateway**



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

На управляющем узле scloud откроем файл /etc/hosts:

Внесем в него следующие записи, после записей 127.0.0.1, но до адресов IPv6:

# Local Addresses a components of the OpenNebula Cloud

192.168.44.130 scloud.PAV.bstu.by scloud one-srv one sunstone

st-serv one-web

192.168.44.131 virt-node.PAV.bstu.by virt-node node1 kvm1

192.168.44.0 swvmnet8

192.168.44.2 gw

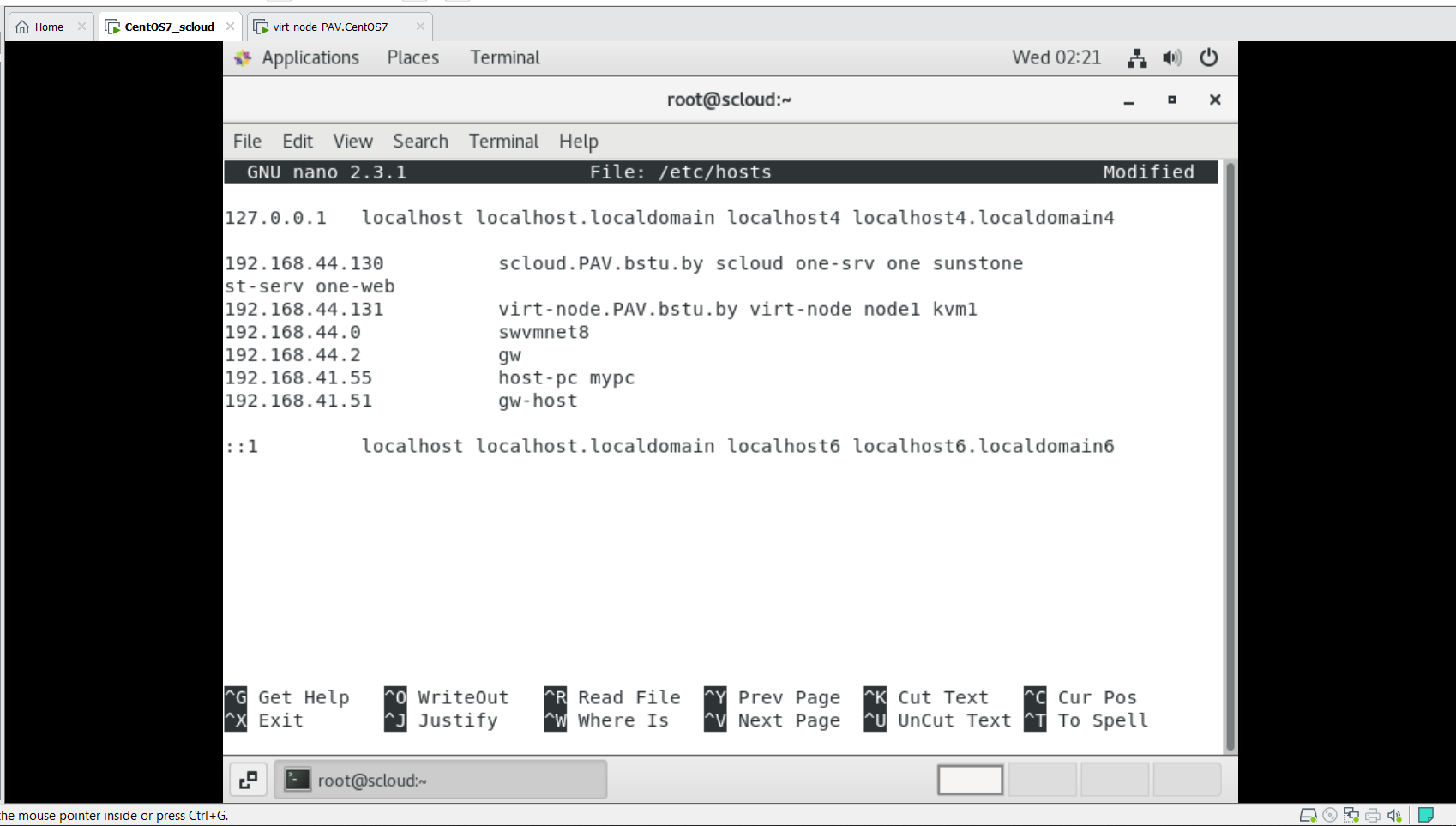
192.168.41.55 host-pc mypc

192.168.41.51 gw-host

Примечение. В качестве разделителя имен могут использоваться следующие знаки:

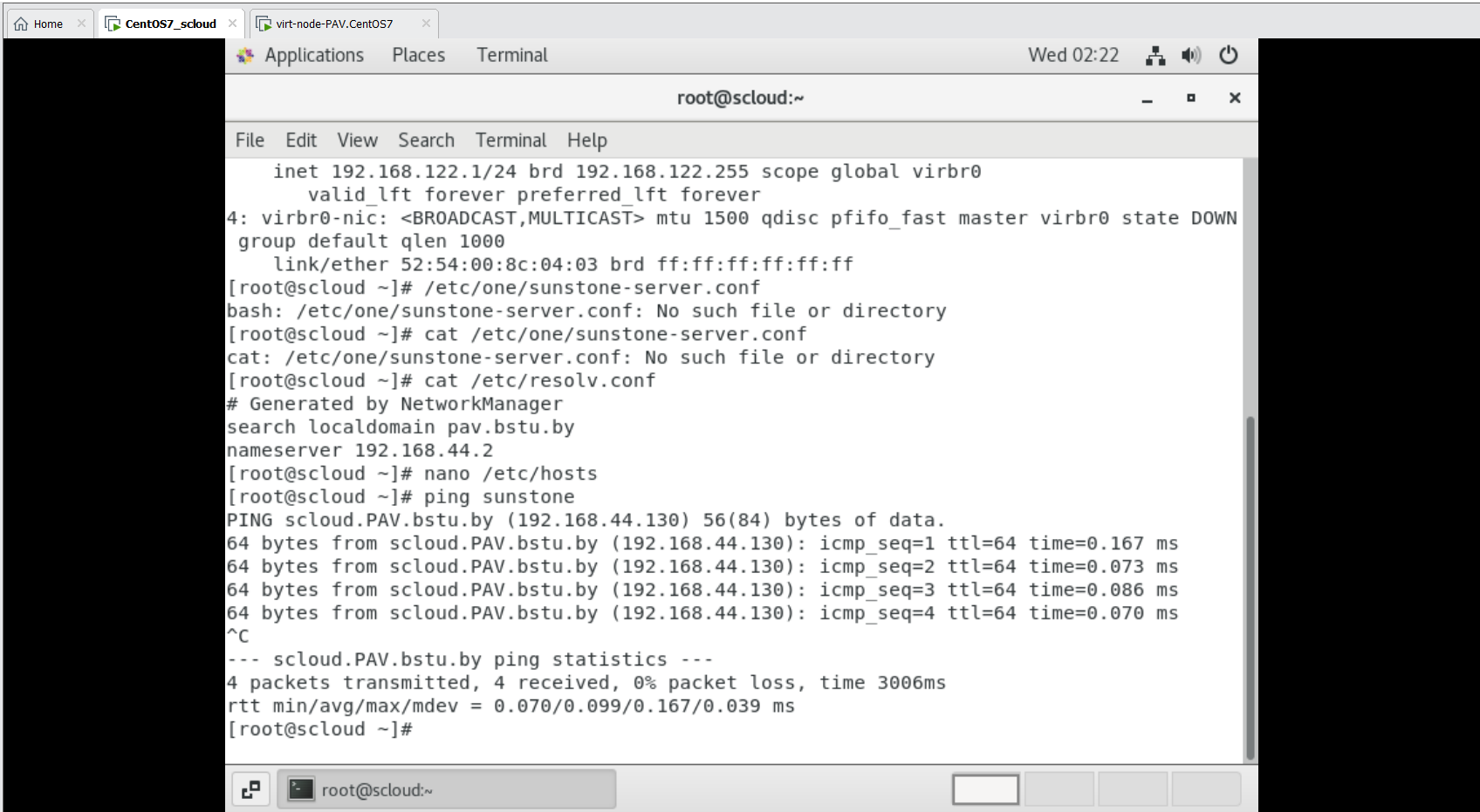
- “ “ (один или несколько пробелов)

- или знак Tab.



Сохраните файл /etc/hosts.

Проверить правильность назначения имен можно с помощью команды ping:



Содержание отредактированного файла /etc/hosts в дальнейшем надо скопировать на все остальные узлы инфраструктуры, создаваемого облака, включая хозяйскую машину (в ОС Windows это файл находится в папке:

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

Как это сделать (смотри ниже п.6) подраздела 1.4.1.

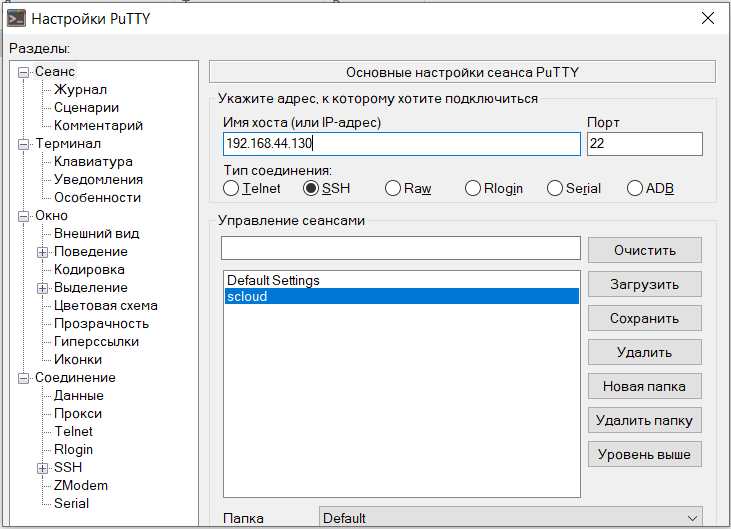
**1.4. Настроить работу службы сервер SSH на главном и рабочем узлах предназначенных для развертывания ОН**

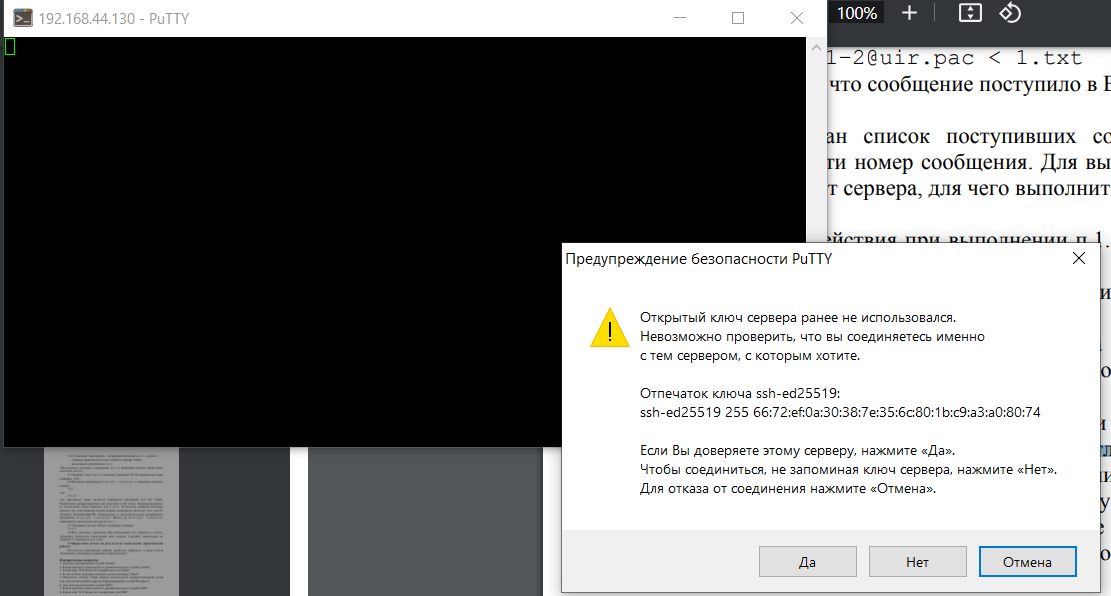
Описанные ниже процедуры выполняются на обеих ВМ, предназначенных для развертывания ПО Opennebula

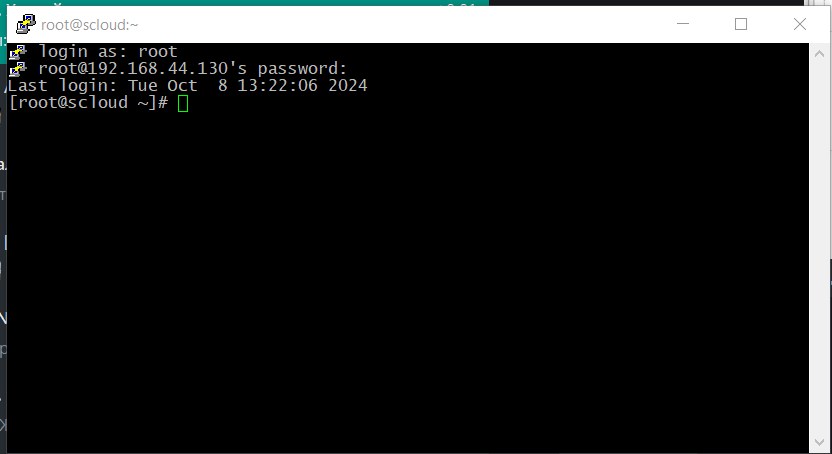
**1.4.1 Знакомство со средствами удаленного администрирования узлов сетевой инфраструктуры облаков.**

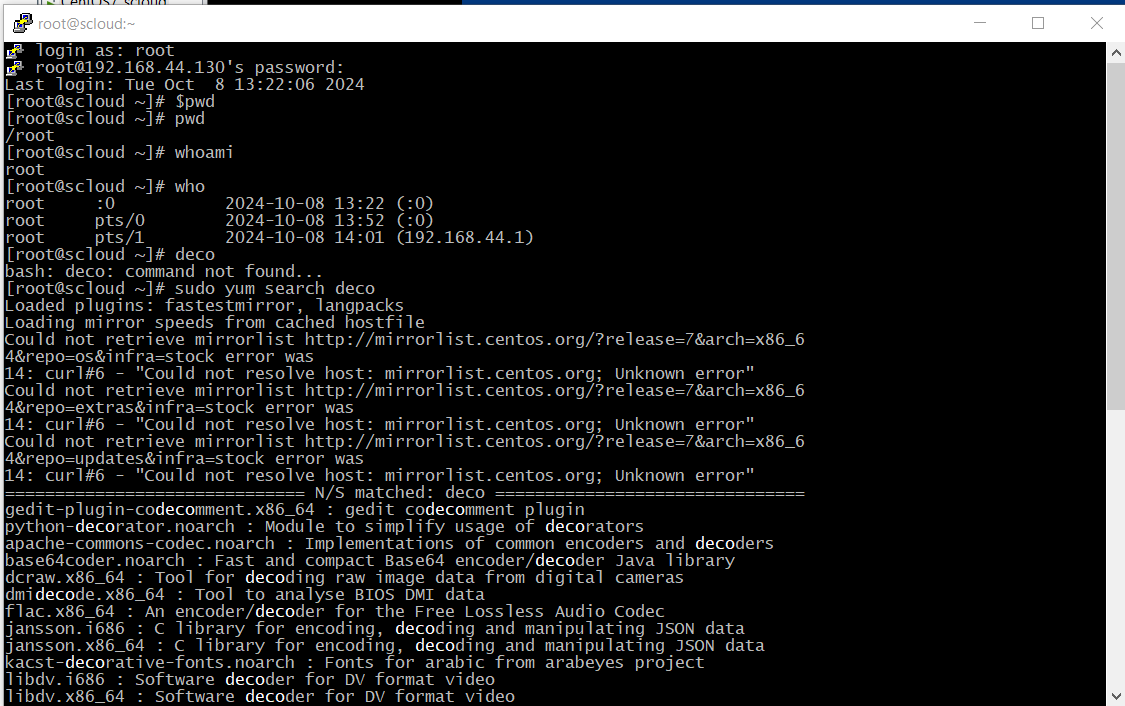
Выполните лабораторную работу 3.1 Telnet и SSH в части касающейся протокола SSH.

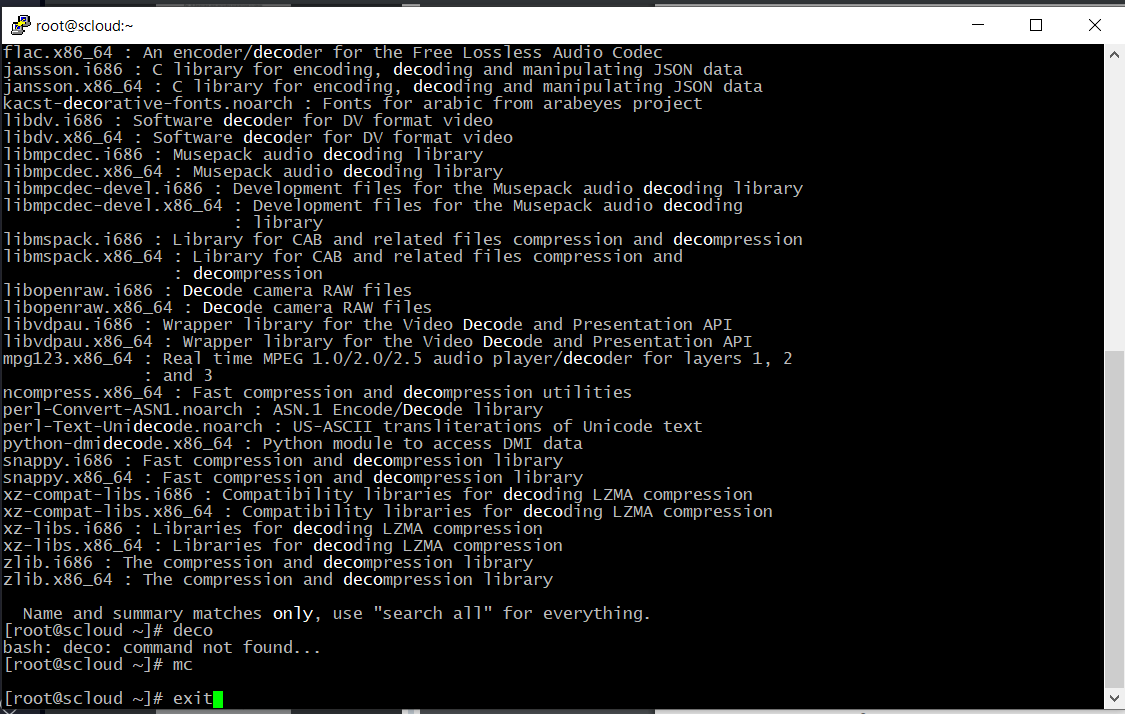
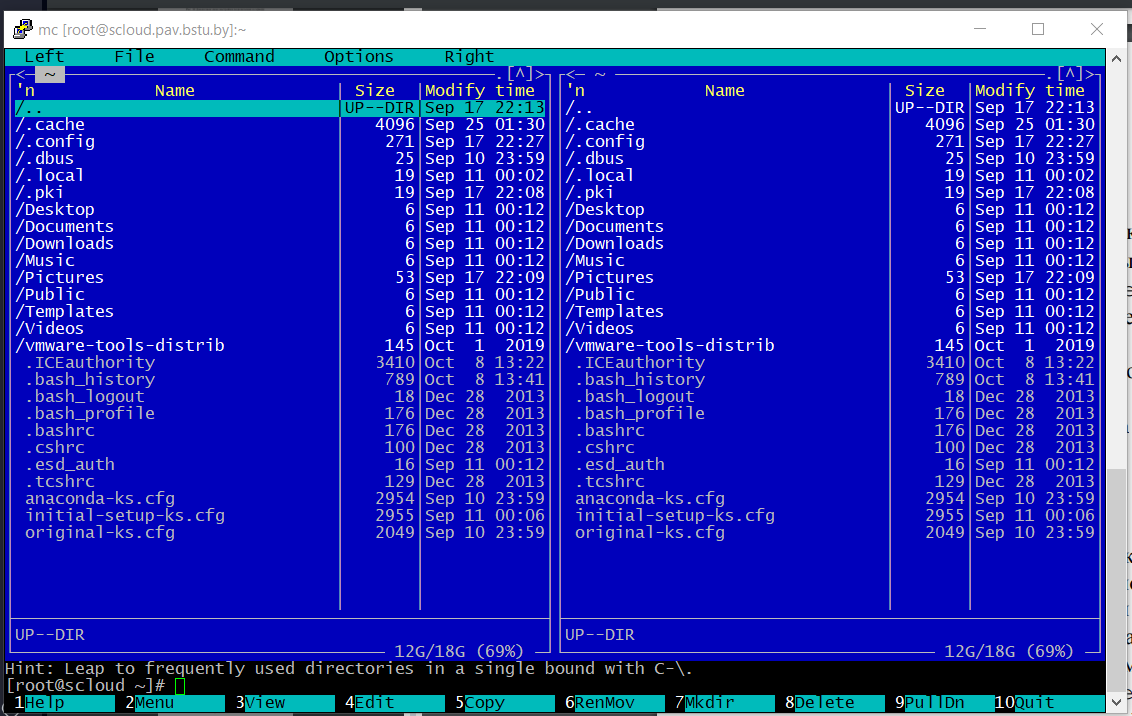
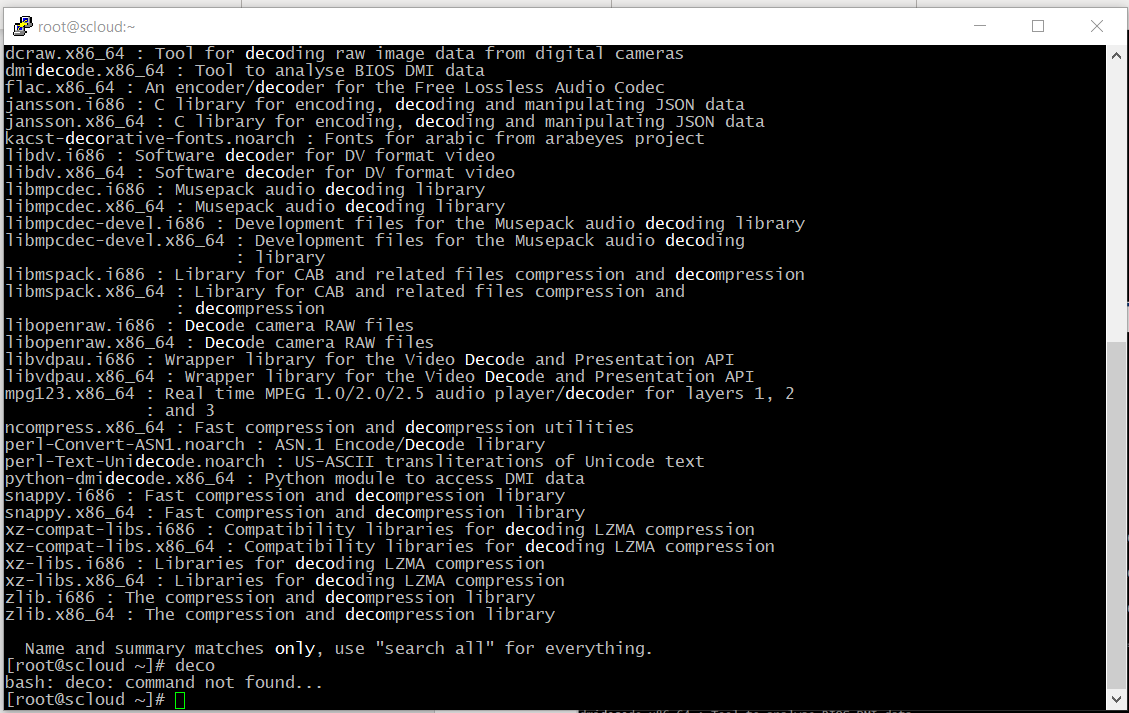
Скачайте из Internet и установите на хозяйскую машину (это Ваша Windows машина) программу клиент SSH Putty. Самостоятельно ознакомьтесь с ее интерфейсом порядком работы с ней.





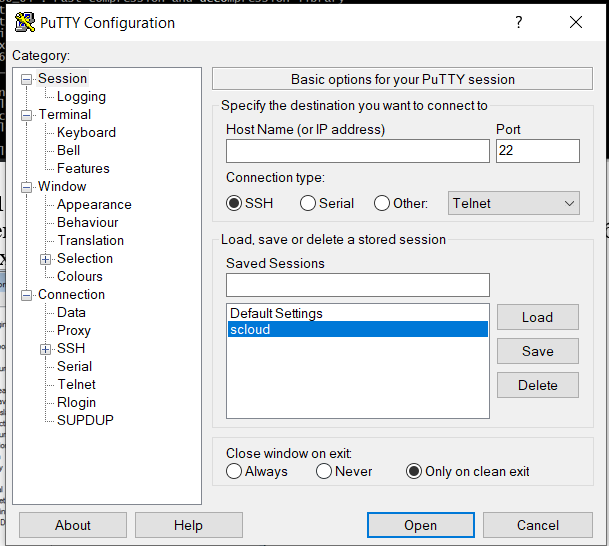






**1.4.1.1 Рекомендации по настройке Putty**

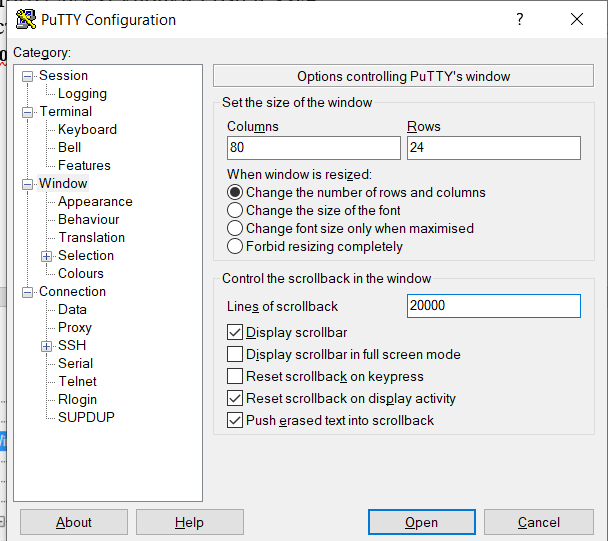
1) Всегда создавайте сохраненные сессии для работы с узлами требующими частых подключений:



Для этого служат кнопки Load и Save.

2) Настройки сессий для корректной работы с Midnight Commander:

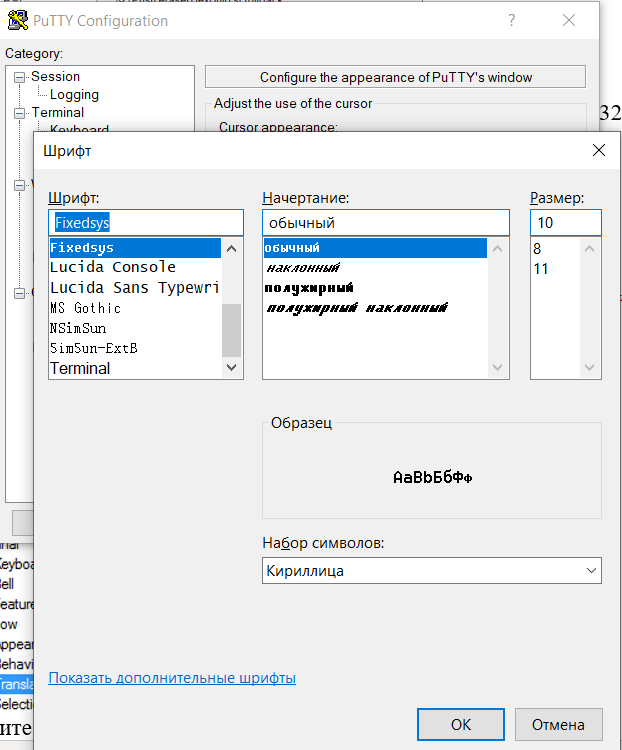
**Window**



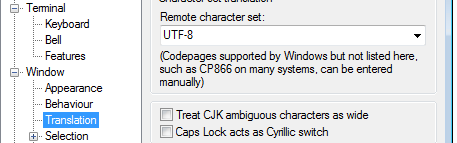
Установите размер буфера прокрутки экрана 20000 и более (макс. 32000)

**Appearance**

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

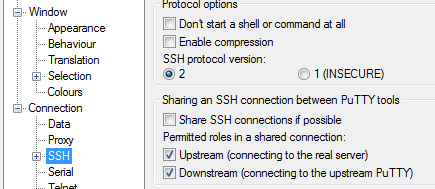


**Translation**



Выберите кодировку UTF-8

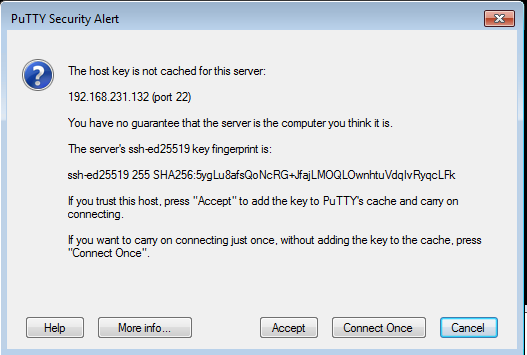
**SSH**



Выберите версию SSH 2

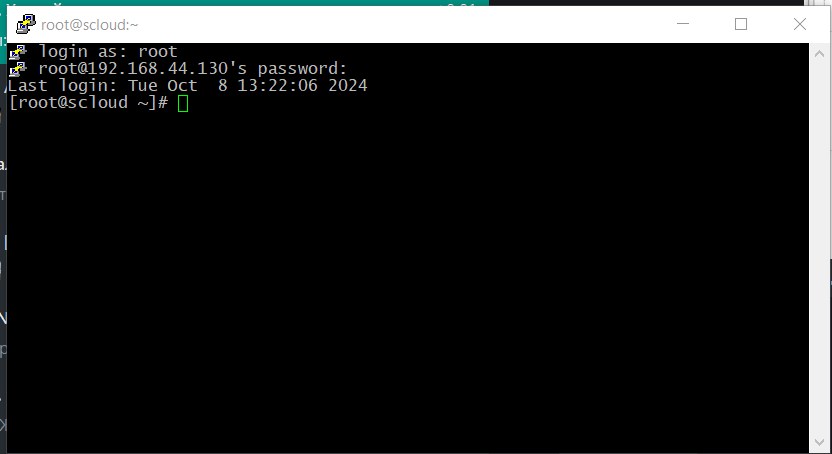
3) Согласование ключей

При первом подключении выдается окно



Для принятия ключей кликните Accept.

Откроется окно терминала в котором надо ввести имя пользователя и пароль.

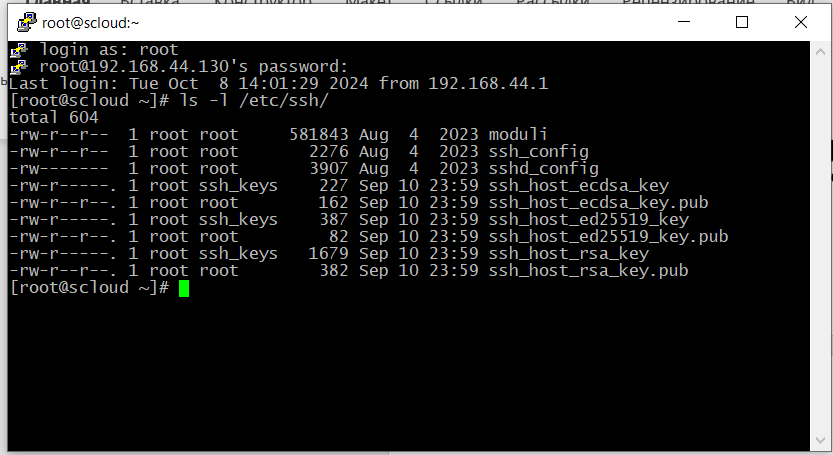


Теперь можно с ВМ scloud имея возможность копировать текст из окна терминала.

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

1) Просмотреть содержимое папки /etc/ssh:

# ls –l /etc/ssh/



Если в этом каталоге нет конфигурационного файла sshd\_config, то сервер SSH не установлен. Для установки необходимо выполнить п. 2), если этот файл есть то надо перейти к п. 3)

2) Установить пакет OpenSSH

# yum install ssh openssh-server

**1.4.2.1 Настройка сервера SSHd**

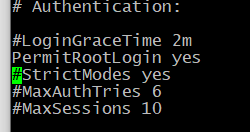
Для этого откройте файл в редакторе nano файл /etc/sshd\_config

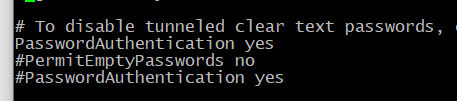
# nano /etc/ssh/sshd\_config

Раскомментируйте строки:

PermitRootLogin yes

PasswordAuthentication yes

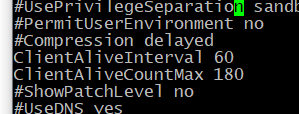


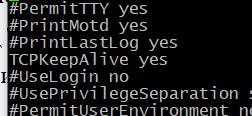


Во всех ОС в целях безопасности устанавливается тайм-аут неактивной работы пользователя, по истечение которого интерфейс пользователя блокируется и ему предлагается пройти аутентификацию для продолжения работы. Для изменения этого времени настроим тайм-аут при работе с использованием SSH надо Найти,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









Теперь, сессия SSH не будет быстро разрываться, пока вы думаете, читаете материалы лаб.работы или работаете над отчетом.

Сохранить файл /etc/ssh/sshd\_config

Выполнив: Ctr+x, y, Enter.

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

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

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



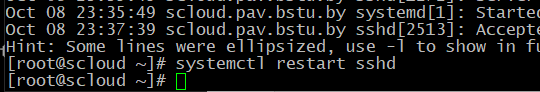
Если команда вернула строку «systemd», значит наши предположения верны.

2) Проверим запущена ли служба сервера SSHD

# systemctl status sshd

Из него следует, что сервис sshd запущен, и его надо просто перезапустить, чтобы внесенные изменения вступили в силу:

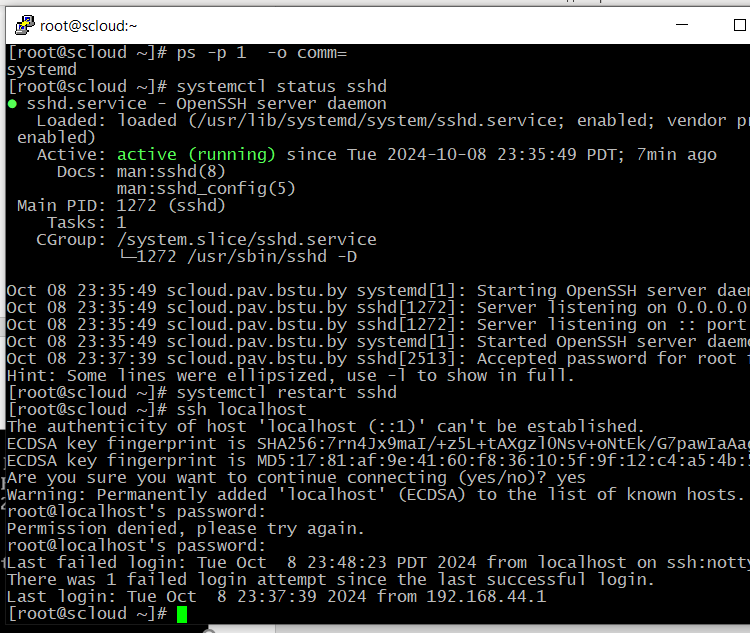
# systemctl restart sshd



3) Проверить работу служб SSHD на обоих узлах:

На управляющем выполнить подключение к самому себе:

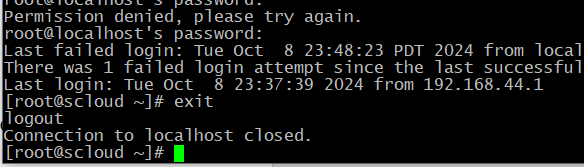
# ssh localhost



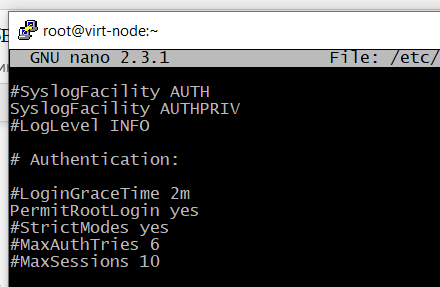
Должен произойти обмен ключами безопасности, потом должен быть запущен процесс проверки пароля, и если все будет правильно выполнено, то откроется сессия SSH (как показано на рис выше).

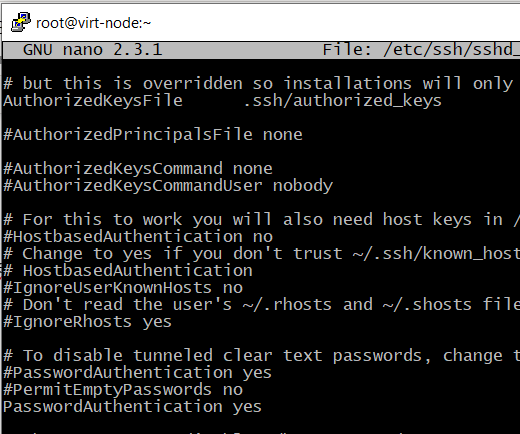
Для выхода из сессии SSH надо ввести:

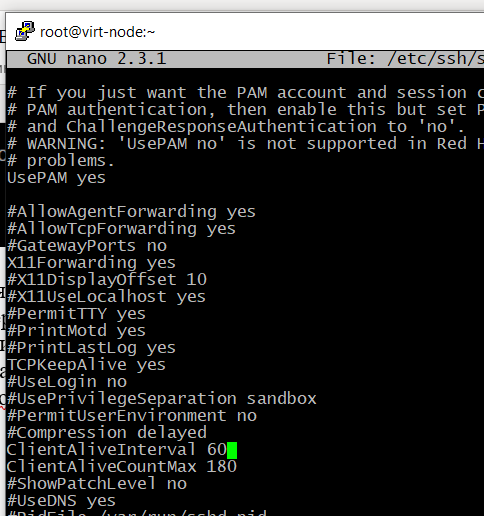
# exit

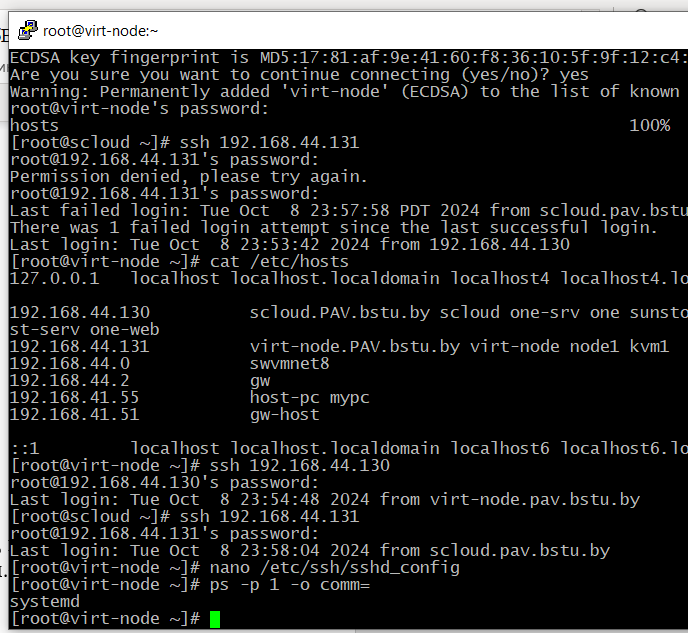


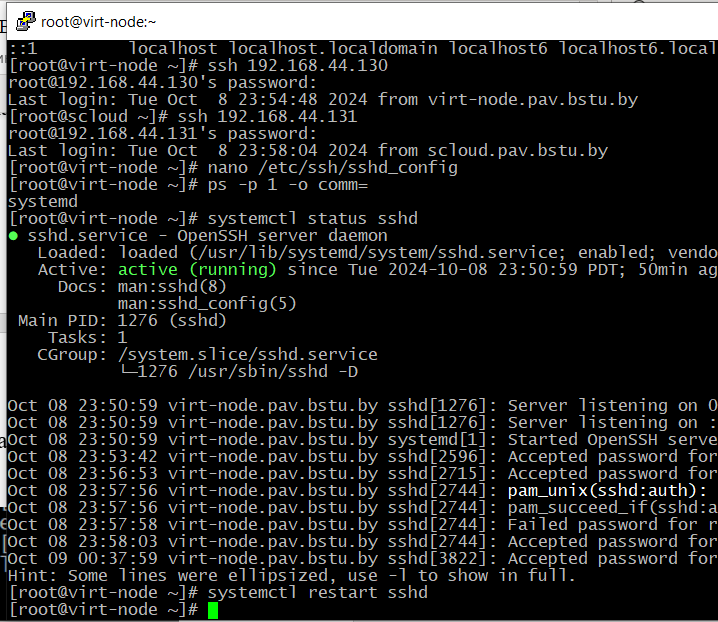
Эту же процедуру необходимо выполнить на рабочем узле virt-node

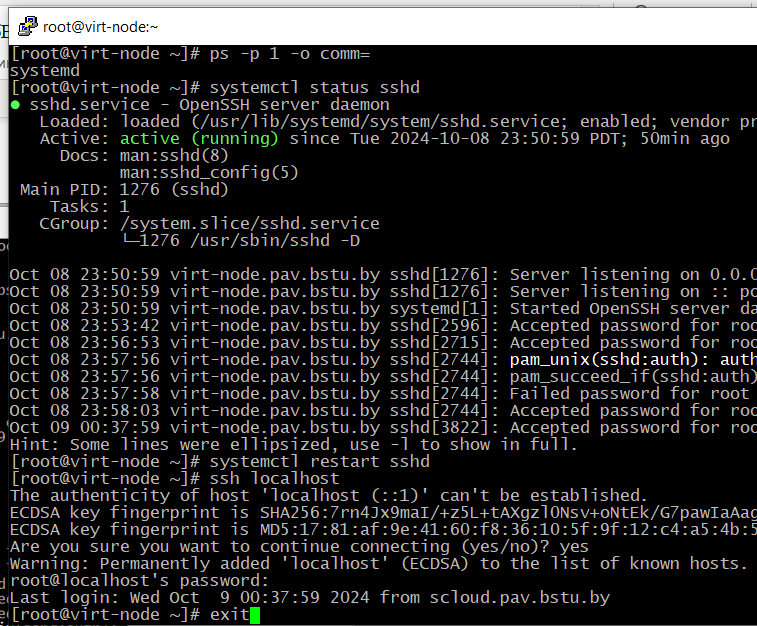








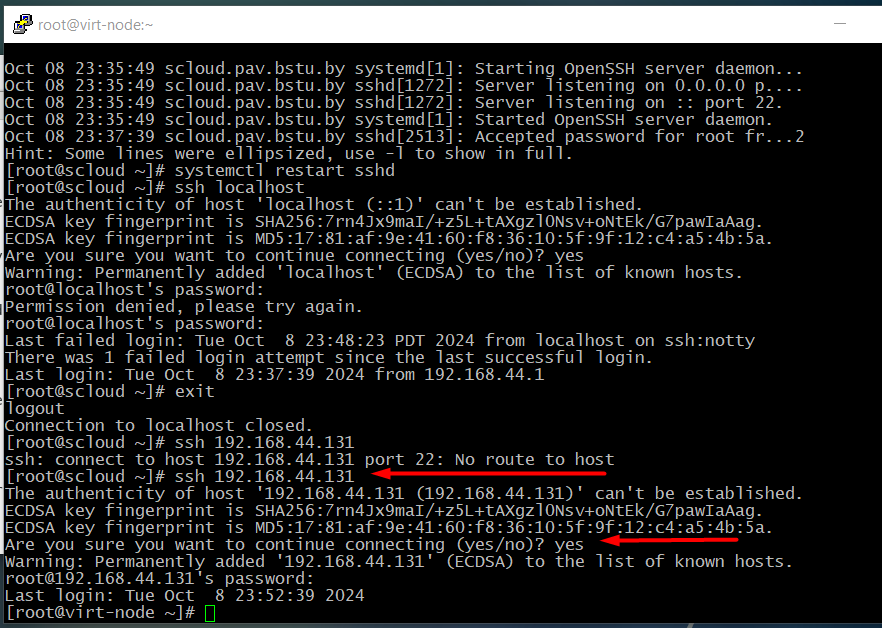




4) Если подключения к самому себе проходят, то надо проверить возможность подключения узлов друг другу в обоих направления.

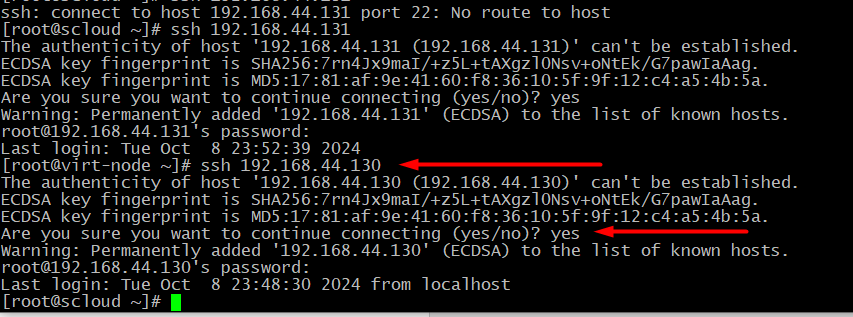
С узла scloud:

# ssh 192.168.44.131



С узла virt-node:

# ssh 192.168.44.130



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

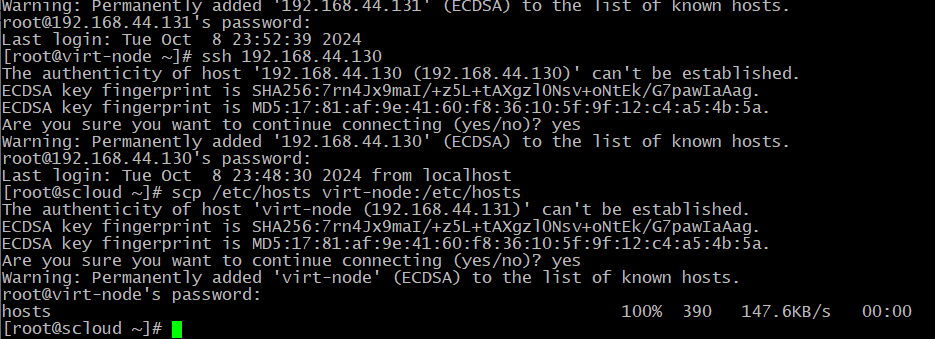
**1.4.3 Копирование файла /etc/hosts на рабочий узел и хозяйскую машину.**

Сейчас можно скопировать файл /etc/hosts подготовленный на узле scloud, на узел virt-node с помощью протокола scp (SSH Copy Protocol) и хозяйскую машину.

Копирование на рабочий узел.

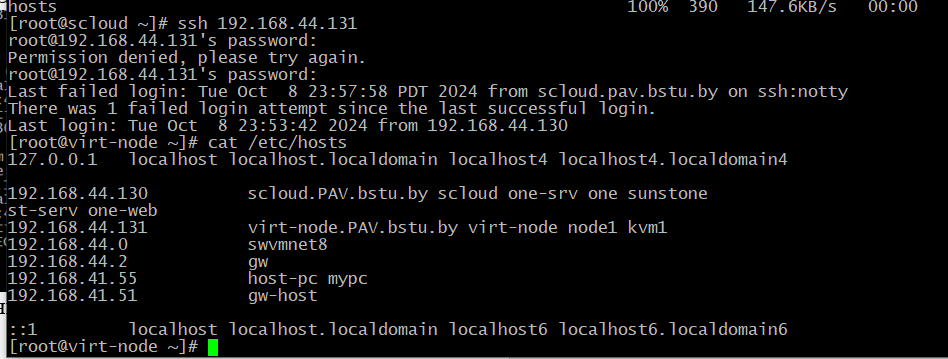
На машине scloud выполнить команду:

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



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

# cat /etc/hosts



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 (предполагается, что она уже установлена на хозяйской машине, если нет то ее следует установить).

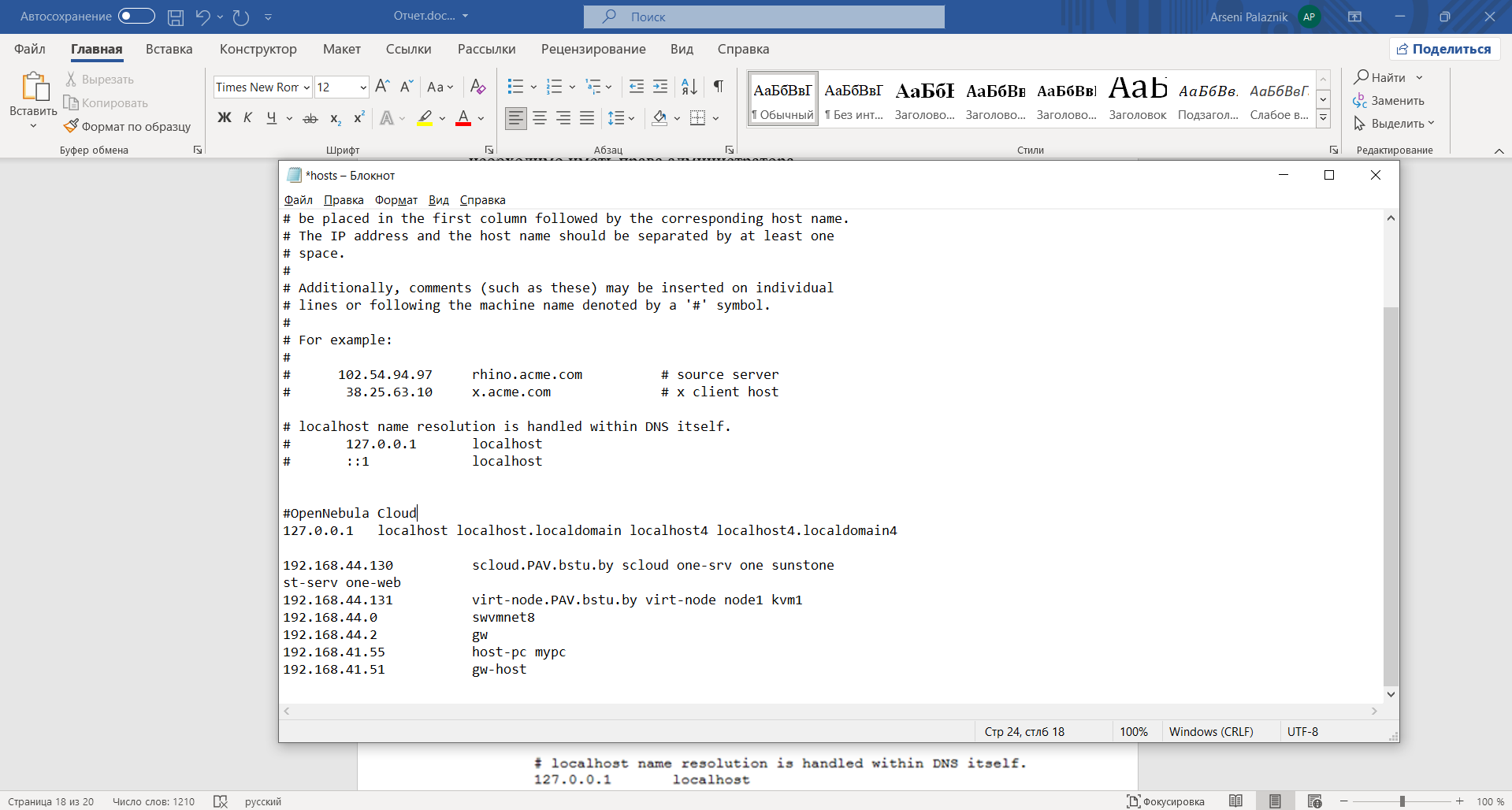
Примечание. Для внесения изменений в файл hosts на хозяйской машине необходимо иметь права администратора.

f) Далее нужно выполнить:

- используя эту программу, скопируйте файл /etc/hosts в свою папку на хозяйской машине;

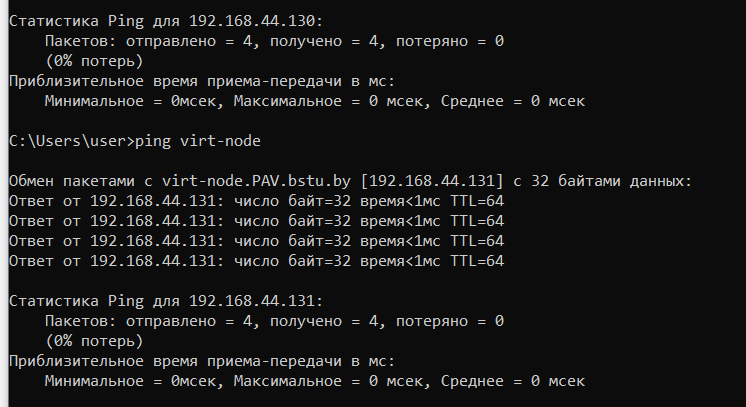
- открыть в редакторе локальный файл c:\Windows\System32\drivers\etc\hosts;

- скопировать в локальный файл hosts записи об именах облачных машин из экспортированного файла hosts и раскомментировать записи localhost;



- сохраните с изменениями локальный файл hоsts в каталоге c:\Windows\System32\drivers\etc\ под именем hosts (без расширения!);

g) проверьте правильность настройки локальных имен с помощью команды ping из хозяйской машины.



После настройки локальных SSH подключений и тиражирования файла hosts между машинами нашей облачной среды можно приступать к установке ПО OpenNebula (см. Лр. 4)

**Итоги**

Подготовлены ВМ узла управления и рабочего узла к развертыванию ПО OpenNebula.

Изучены важнейшие средства удаленного администрирования облачных серверов.

**Вопросы**

**1. Для чего предназначена служба Telnet?**

Telnet предназначен для удаленного управления устройствами и серверами через текстовый интерфейс. Он позволяет пользователям подключаться к удаленным системам и выполнять команды так, как если бы они работали непосредственно на этих системах.

**2. Какой протокол транспортного уровня использует служба Telnet?**

Telnet использует протокол TCP (Transmission Control Protocol) для установления соединений.

**3. Какой порт TCP является стандартным для Telnet?**

Стандартным TCP портом для Telnet является порт 23.

**4. В чем состоит основная опасность использования Telnet?**

Основная опасность использования Telnet заключается в отсутствии шифрования данных. Все передаваемые данные, включая логины и пароли, передаются в открытом виде, что делает их уязвимыми для перехвата и атак типа "человек посередине".

**5. Объясните, почему Telnet широко используется администраторами сетей для диагностики работы других информационных служб Интернет?**

Telnet используется администраторами сетей для диагностики и тестирования соединений, проверки доступности портов и конфигурации сетевых устройств. Он позволяет быстро и просто подключаться к удаленным системам и выполнять команды для проверки их состояния.

**6. Для чего предназначена служба SSH?**

SSH (Secure Shell) предназначен для безопасного удаленного управления устройствами и серверами. Он обеспечивает шифрование данных, что делает соединения защищенными от перехвата

**7. Какой протокол транспортного уровня использует служба SSH?**

SSH также использует протокол TCP для установления соединений

**8. Какой порт TCP является стандартным для SSH?**

Стандартным TCP портом для SSH является порт 22

**9. Кратко расскажите о возможностях программы PuTTY.**

PuTTY — это бесплатный клиент для SSH и Telnet, который позволяет пользователям подключаться к удаленным серверам и управлять ими через командную строку. Он поддерживает различные протоколы, включая SSH, Telnet, SCP и SFTP, и предоставляет удобный интерфейс для настройки соединений

**10. Каково назначение и основные функции программ deco и Midnight Commander (mc)?**

- Deco: Это текстовый редактор и файловый менеджер для Unix-подобных систем, который позволяет пользователям редактировать файлы и управлять каталогами.

- Midnight Commander (mc): Это мощный файловый менеджер с текстовым интерфейсом, который позволяет пользователям копировать, перемещать, удалять файлы и каталоги, а также выполнять другие операции с файлами.

**11. С помощью каких клавиш в командных оболочках deco и mc выполняются следующие действия:**

- Выделение файлов и каталогов: В mc используется клавиша Insert.

- Копирование файлов и каталогов: В mc используется клавиша F5.

- Перемещение файлов и каталогов: В mc используется клавиша F6.

- Удаление файлов и каталогов: В mc используется клавиша F8.

- Создание каталогов: В mc используется клавиша F7.

- Редактирование файлов: В mc используется клавиша F4.

- Получение справки по функциям данных программ: В mc используется клавиша F1.

- Поиск в файлах заданных подстрок: В mc используется клавиша F7 для поиска.

**Deco:**

- Выделение файлов и каталогов: В deco используется клавиша Insert.

- Копирование файлов и каталогов: В deco используется клавиша F5.

- Перемещение файлов и каталогов: В deco используется клавиша F6.

- Удаление файлов и каталогов: В deco используется клавиша F8.

- Создание каталогов: В deco используется клавиша F7.

- Редактирование файлов: В deco используется клавиша F4.

- Получение справки по функциям данных программ: В deco используется клавиша F1.

- Поиск в файлах заданных подстрок: В deco используется клавиша ctrl + f или ctrl + shift + f для поиска.

**V. Подготовка отчета**

**1. Подготовить отчет о выполнении данной работы.**

1.1 В отчет включите описание всех выполненных действий (раздел 1. Выполнение работы).

1.2. Также в отчет необходимо включить ответы на контрольные вопросы (раздел 2. Ответы на контрольные вопросы).

**V. Контрольные вопросы**

Включите в отчет ответы на контрольные вопросы, приведенные в Л.р.3.1 и касающиеся протокола SSH.

**VI. Защита отчета**

**1. Предъявите отчет преподавателю для защиты.**