## Учреждение образования

## Белорусский государственный технологический университет

Кафедра информационных систем и технологий

**ЛАБОРАТОРНАЯ РАБОТА 3**

по дисциплине «Облачные технологии»

Выполнил студент

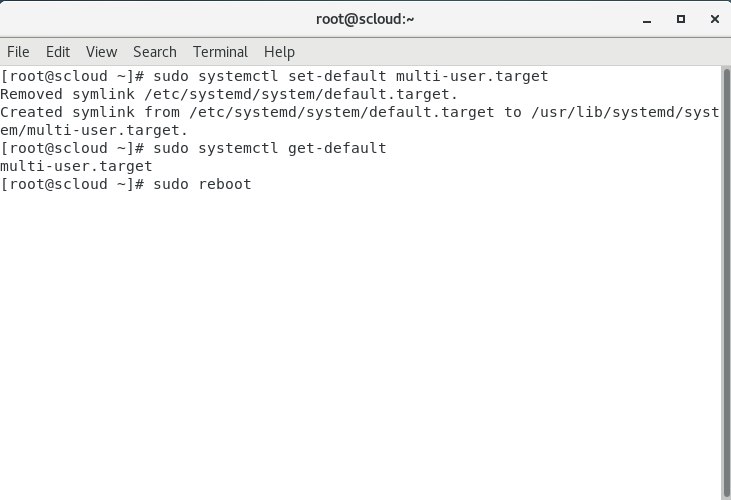
Бобрович Г.С.

Минск 2024

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

Описанные ниже действия необходимо выполнить на ВМ главного и рабочего узлов, работающих под ОС CentOS 7 до начала установки ПО Opennebula.

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



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

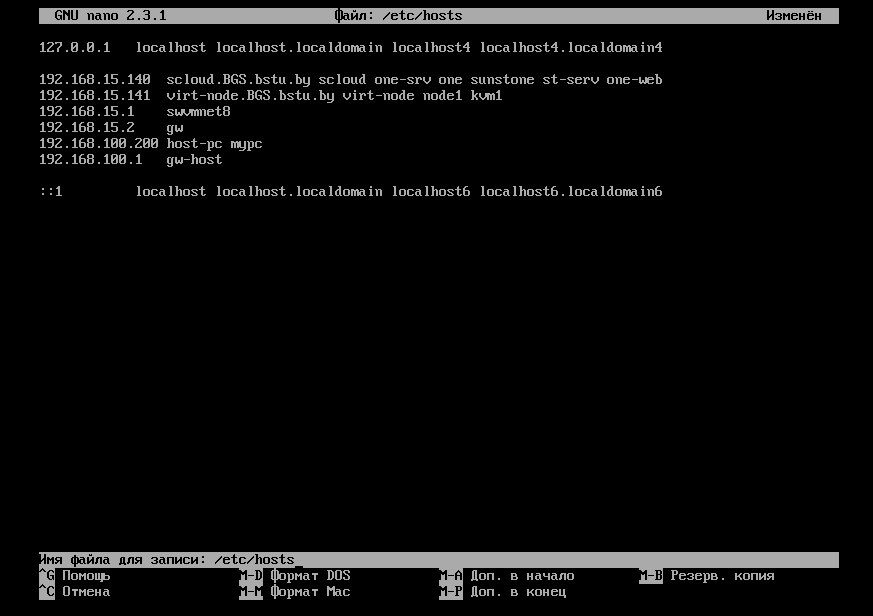
Если при выполнении лабораторной работы вы работаете с использование сетевого подключения в компьютерном классе, в котором доступ машин к Интернет реализуется через прокси, то необходимо выполнить следующие настройки пользовательского окружения в ОС ВМ головного и рабочего хостов ОН (Орен Небула).

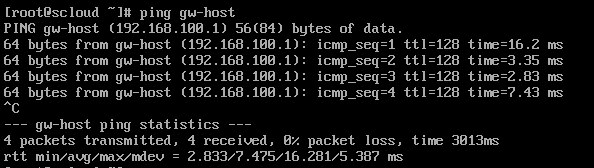
Замечание. Если Ваш доступ к Интернет не требует использования прокси-сервера, то п.1.2.1 выполнять не надо.

**1.3.1 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:



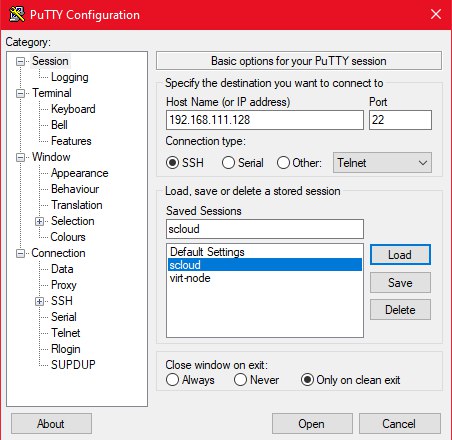


**1.4. Настроить работу службы сервер SSH на главном и рабочем узлах предназначенных для развертывания ОН**

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

**1.4.1.1 Рекомендации по настройке Putty**

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



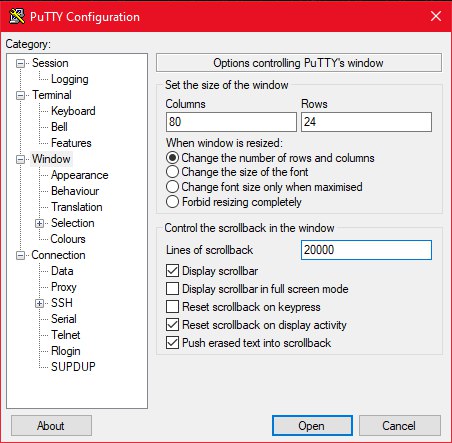
Для этого служат кнопки Load и Save.

2) Настройки сессий для корректной работы с Midnight Commander:

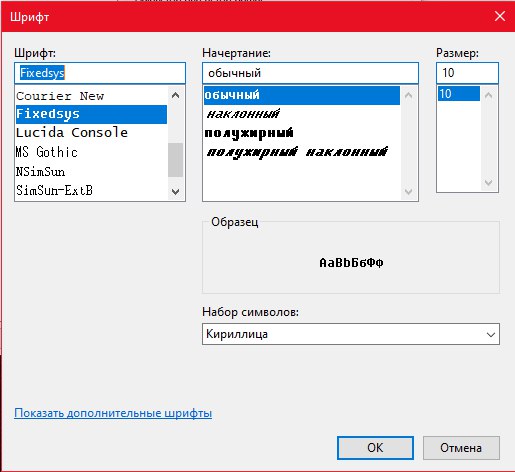
**Window**

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

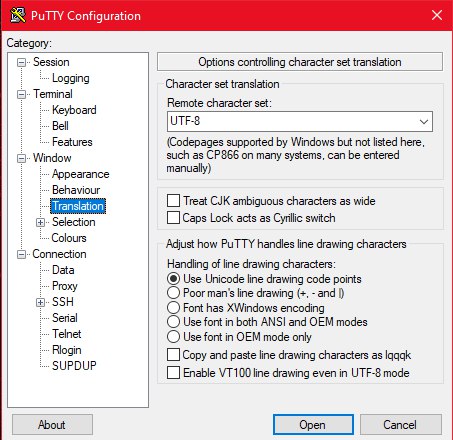
**Appearance**



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

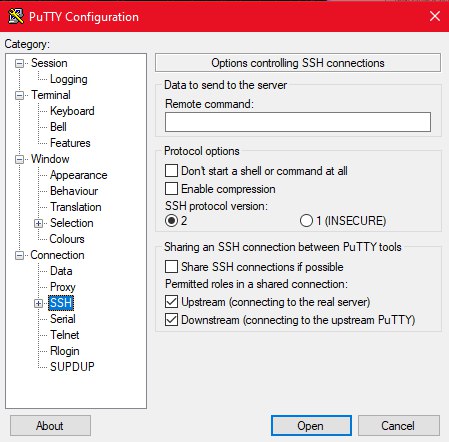


**Translation**



Выберите кодировку UTF-8

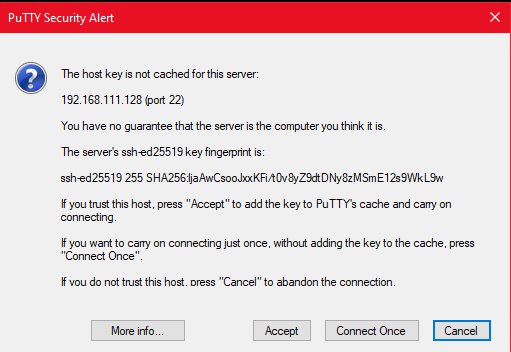
**SSH**



Выберите версию SSH 2

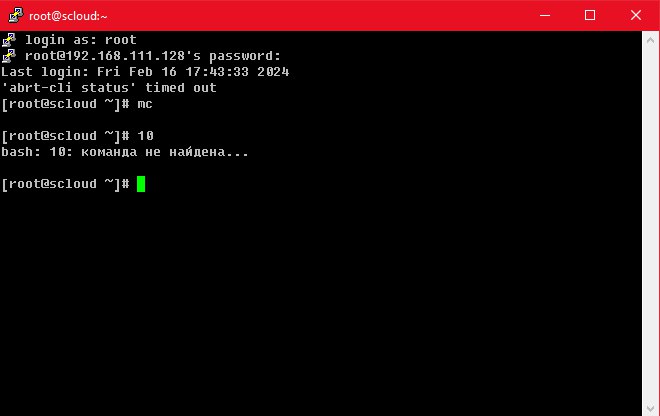
3) Согласование ключей

При первом подключении выдается окно



Для принятия ключей кликните Accept.

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

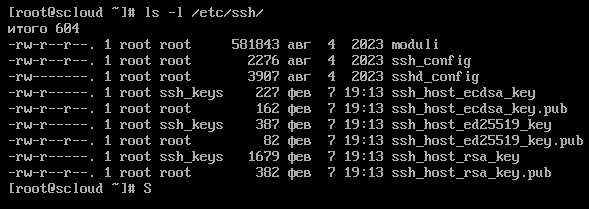


Теперь можно с ВМ scloud имея возможность копировать текст из окна терминала.

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

1) Просмотреть содержимое папки /etc/ssh:

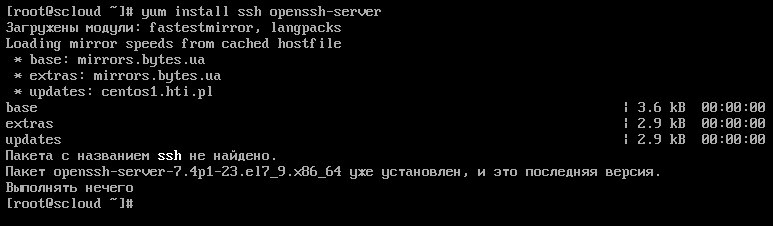
# ls –l /etc/ssh/



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

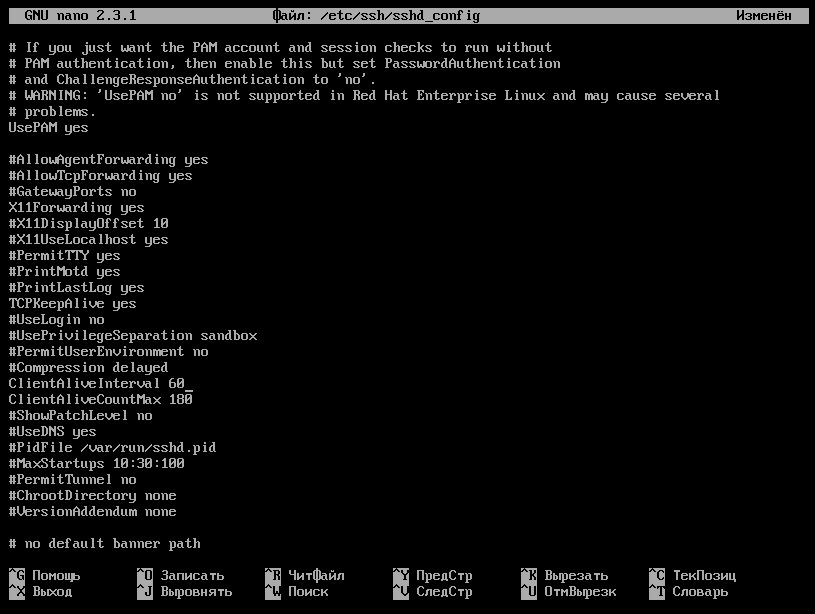
Раскомментируйте строки:

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.

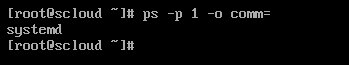
Сохранить файл /etc/ssh/sshd\_config

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:

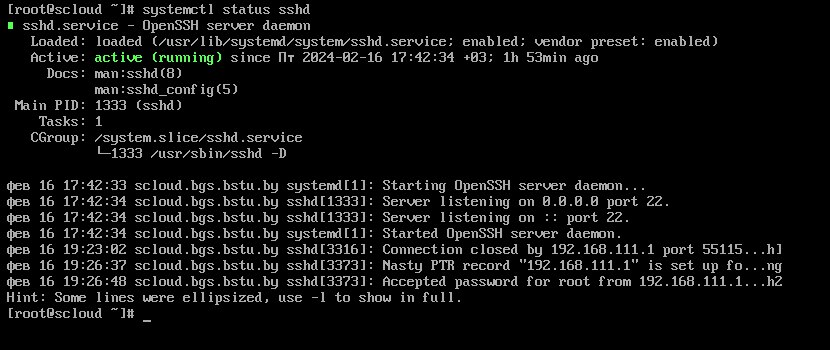
|  |
| --- |
| ps -p 1 -o comm= |



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

2) Проверим запущена ли служба сервера SSHD

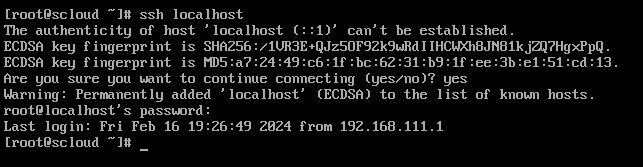
# systemctl status sshd



3) Проверить работу служб SSHD на обоих узлах:

На управляющем выполнить подключение к самому себе:

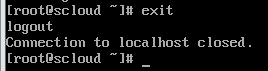
# ssh localhost



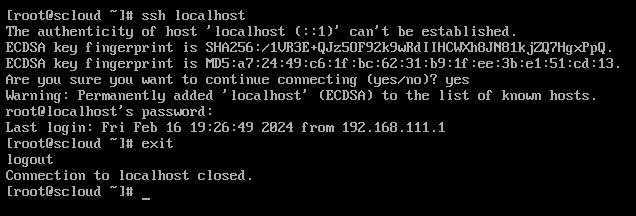
Должен произойти обмен ключами безопасности, потом должен быть запущен процесс проверки пароля, и если все будет правильно выполнено, то откроется сессия SSH (как показано на рис выше).

Для выхода из сессии SSH надо ввести:

# exit



Эту же процедуру необходимо выполнить на рабочем узле virt-node



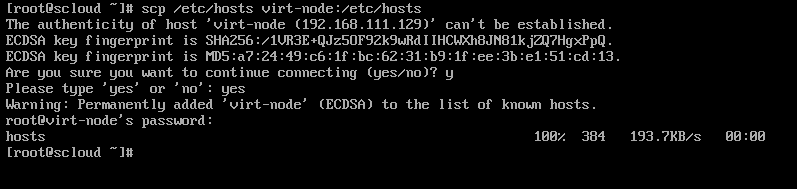
**1.4.3 Копирование файла /etc/hosts на рабочий узел и хозяйскую машину.**

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

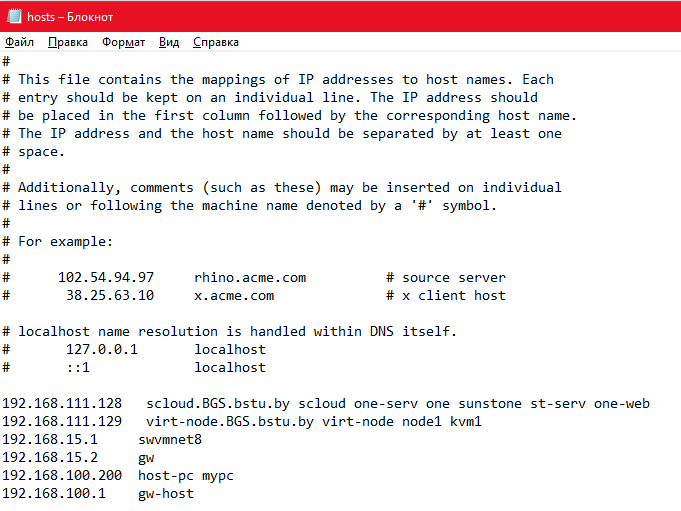
Копирование на рабочий узел.

На машине scloud выполнить команду:

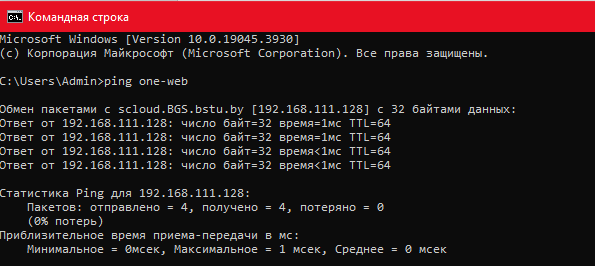
# scp /etc/hosts virt-node:/etc/hosts



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



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



**Итоги**

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

Изучены важнейшие средства удаленного администрирования облачных серверов.

**V. Контрольные вопросы**

1. Telnet предназначен для обеспечения двусторонней интерактивной связи между компьютерами в интернете и локальных сетях. Он позволяет пользователям подключаться к удаленным системам и выполнять задачи, как если бы они находились перед этим компьютером.

2. Telnet использует протокол транспортного уровня TCP.

3. Стандартный порт TCP для Telnet - это порт 23.

4. Основная опасность использования Telnet заключается в том, что он передает все данные, включая имена пользователей и пароли, в открытом виде. Это делает его небезопасным для использования в чувствительных к безопасности приложениях.

5. Telnet широко используется администраторами сетей для диагностики работы других информационных служб Интернет, потому что он позволяет устанавливать соединение с удаленной системой и выполнять задачи, как если бы они находились перед этим компьютером.

6. SSH (Secure Shell) - это протокол, предназначенный для безопасного удаленного входа с одного компьютера на другой. Он обеспечивает сильную аутентификацию и защищает безопасность и целостность коммуникаций с помощью сильного шифрования.

7. SSH использует протокол транспортного уровня TCP.

8. Стандартный порт TCP для SSH - это порт 22.

9. PuTTY - это бесплатный и открытый терминальный эмулятор, консоль последовательного соединения и приложение для передачи файлов по сети. Он поддерживает несколько сетевых протоколов, включая SCP, SSH, Telnet, rlogin и raw socket connection. Он также может подключаться к последовательному порту.

10. Midnight Commander (mc) - это текстовый файловый менеджер, который предоставляет двухпанельный интерфейс и множество функций для работы с файлами. Он позволяет пользователям эффективно перемещаться по файловой системе и выполнять различные операции с файлами. О программе deco информация не найдена.

11. В Midnight Commander (mc):

Выделение файлов и каталогов: клавиши вверх и вниз для навигации, Insert для выделения.

Копирование файлов и каталогов: F5.

Перемещение файлов и каталогов: F6.

Удаление файлов и каталогов: F8.

Создание каталогов: F7.

Редактирование файлов: F4.

Получение справки по функциям данных программ: F1.

Поиск в файлах заданных подстрок: Alt + ?.