**Облачные технологии**

Лабораторная работа № 3

**Подготовка виртуальных машин к развертыванию облака OpenNebula**

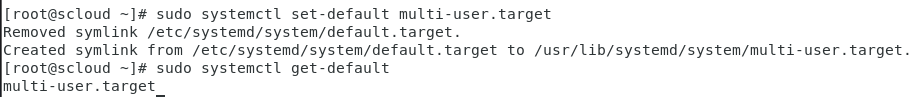
**1. Подготовка виртуальных машин к развертыванию облака OpenNebula**

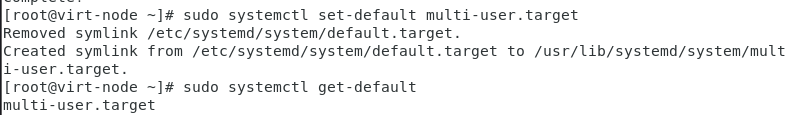
Описанные ниже действия необходимо выполнить на ВМ главного и рабочего узлов, работающих под ОС CentOS 7 до начала установки ПО Opennebula.

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

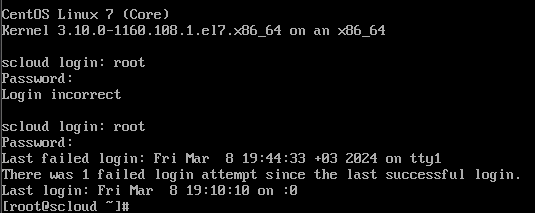
Отключить запуск X-ов при старте системы можно выполнив команду:

проверяем:



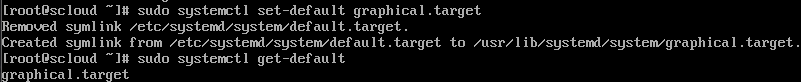


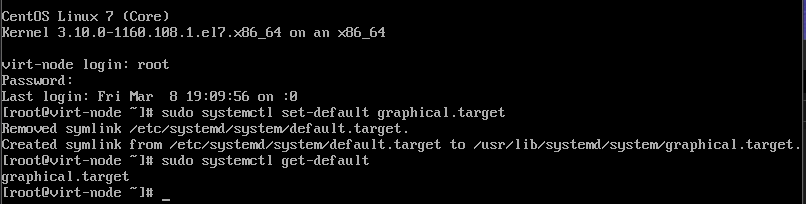
Перезагружаемся без GUI



Вернуть обратно запуск графической оболочки можно с помощью команды:

проверяем:

****

****

**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 | 192.168.17.128/24 | Сервер OpenNebula |
| 2 | **sunstone**  st-serv  one-web |  | Web-сервер Sunstone управления облаком |
| 3 | **virt\_node**  virt-node1  node1  kvm1 | 192.168.17.129/24 | Сервер виртуализации |
| 4 | **swvmnet8** | 192.168.17.0 | 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 | 192.168.178.246 | Хозяйская машина |
| 8 | **gw-host** | 192.168.178.104 | 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

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

На управляющем узле scloud откроем файл /etc/hosts:

# Local Addresses a components of the OpenNebula Cloud

192.168.17.133 scloud.BBB.bstu.by scloud one-srv one sunstone

st-serv one-web

192.168.17.132 virt-node.BBB.bstu.by virt-node node1 kvm1

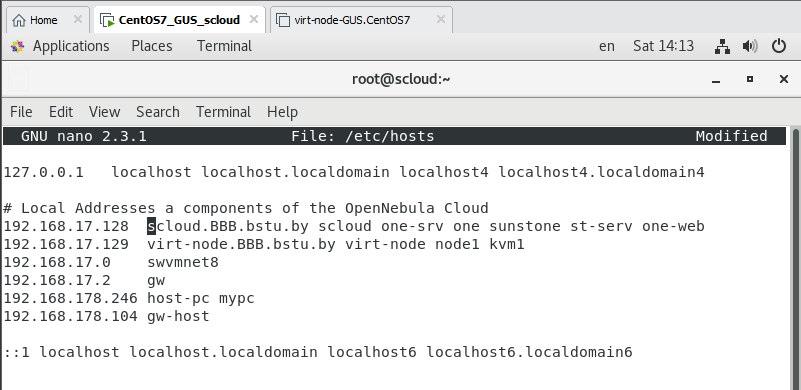
192.168.17.0 swvmnet8

192.168.17.2 gw

192.168.178.246 host-pc mypc

192.168.178.104 gw-host

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



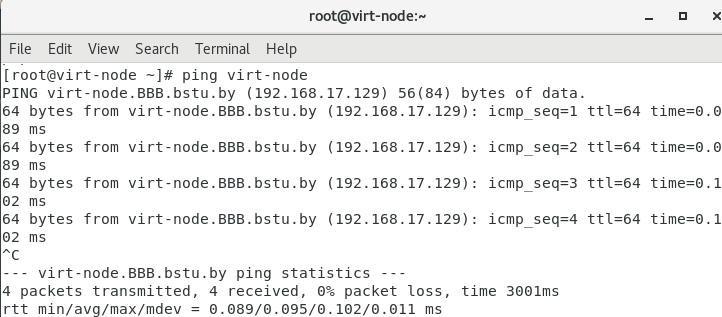
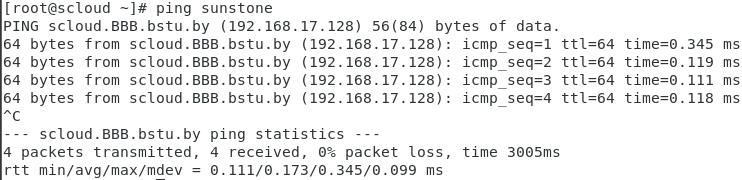
Примечение. В качестве разделителя имен могут использоваться следующие знаки:

- “ “ (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

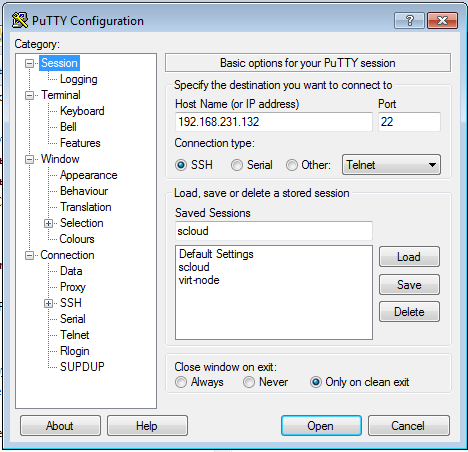
**1.4.1 Знакомство со средствами удаленного администрирования узлов сетевой инфраструктуры облаков.**

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**

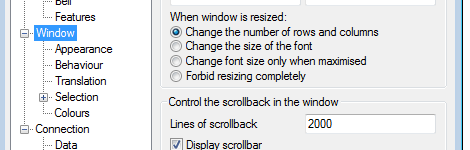
1) Всегда создавайте сохраненные сессии для работы с узлами требующими частых подключений:



Для этого служат кнопки Load и Save.

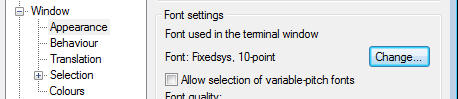
2) Настройки сессий для корректной работы с Midnight Commander:

**Window**

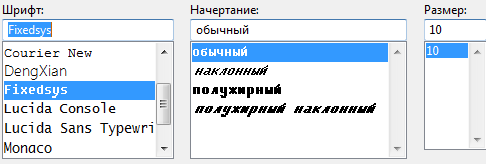


Установите размер буфера прокрутки экрана 20000 и более (макс. 32000)

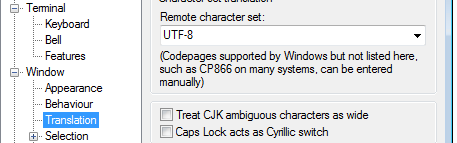
**Appearance**



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

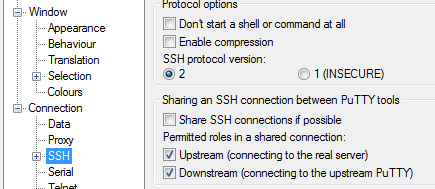


**Translation**



Выберите кодировку UTF-8

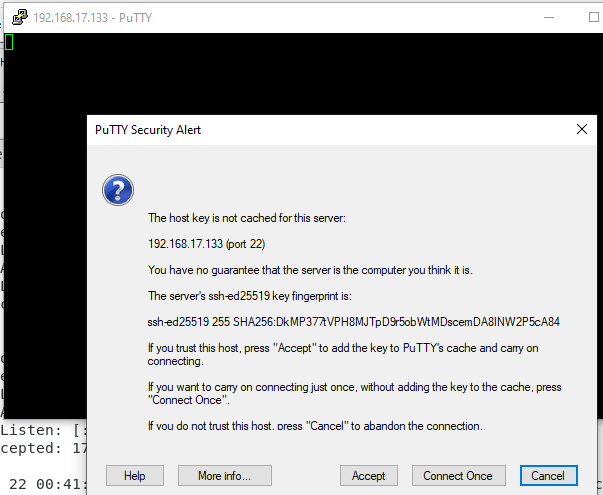
**SSH**



Выберите версию SSH 2

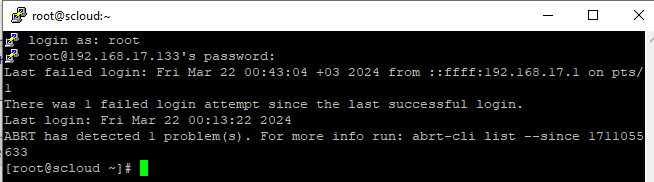
3) Согласование ключей

При первом подключении выдается окно



Для принятия ключей кликните Accept.

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

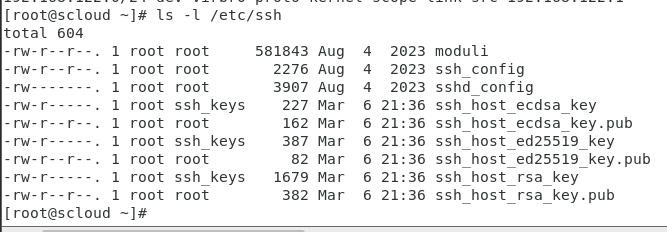


Теперь можно с ВМ scloud имея возможность копировать текст из окна терминала.

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

1) Просмотреть содержимое папки /etc/ssh:

# ls –l /etc/ssh/

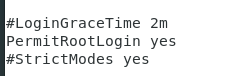
Если в этом каталоге нет конфигурационного файла sshd\_config, то сервер SSH не установлен. 

**1.4.2.1 Настройка сервера SSHd**

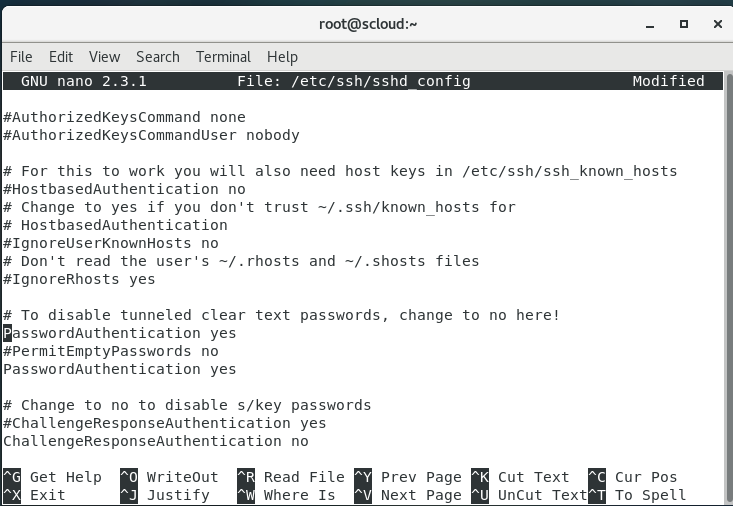
Для этого откройте файл в редакторе nano файл /etc/sshd\_config

# nano /etc/ssh/sshd\_config

Раскомментируйте строки:



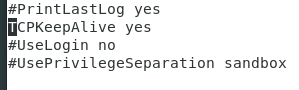
PermitRootLogin yes



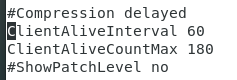
PasswordAuthentication yes

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= |

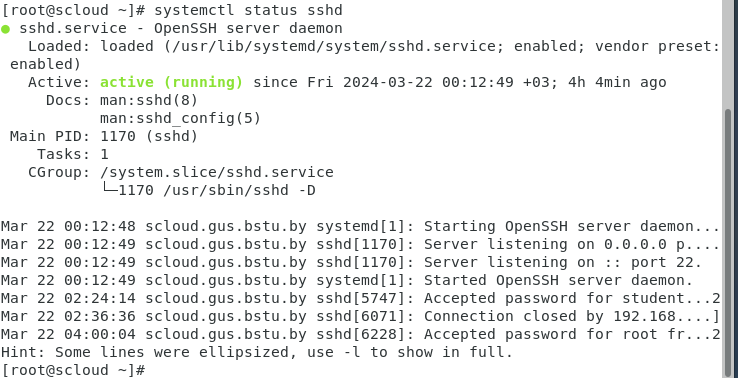


Если команда вернула строку «systemd», значит наши предположения верны.

2) Проверим запущена ли служба сервера SSHD

# systemctl status sshd

Ответ на эту команду должен быть следующим:



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

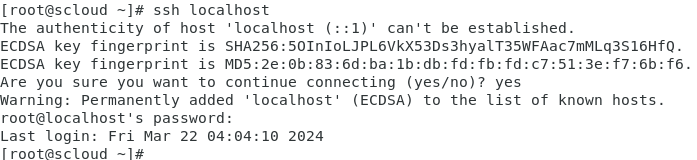
# systemctl restart sshd



3) Проверить работу служб SSHD на обоих узлах:

На управляющем выполнить подключение к самому себе:

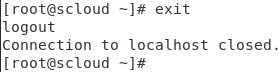
# ssh localhost



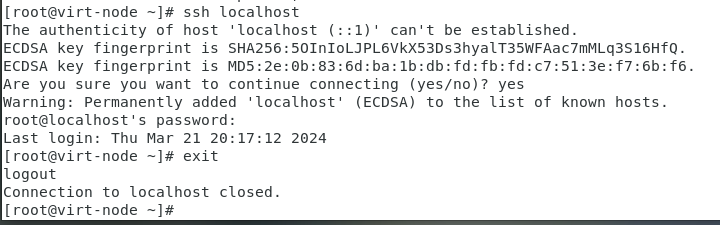
Должен произойти обмен ключами безопасности, потом должен быть запущен процесс проверки пароля, и если все будет правильно выполнено, то откроется сессия SSH (как показано на рис выше).

Для выхода из сессии SSH надо ввести:

# exit



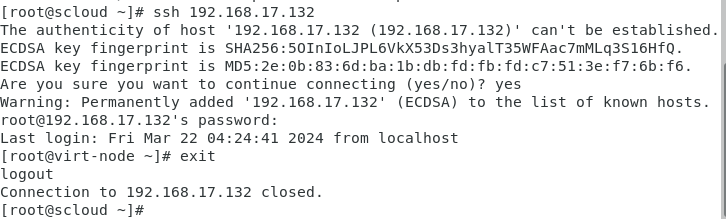
Эту же процедуру необходимо выполнить на рабочем узле virt-node



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

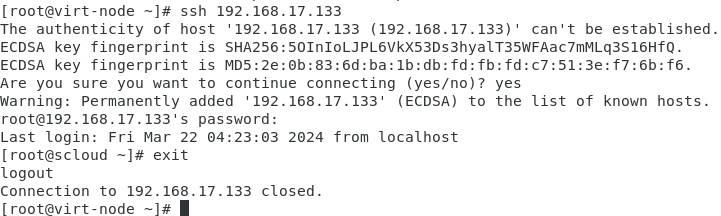
С узла scloud:

# ssh 192.168.15.141



С узла virt-node:

# ssh 192.168.15.140



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

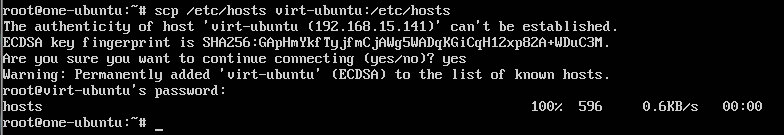
**1.4.3 Копирование файла /etc/hosts на рабочий узел и хозяйскую машину.**

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.

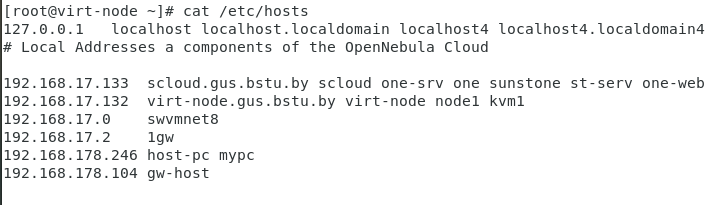
На машине scloud выполнить команду:

# 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.

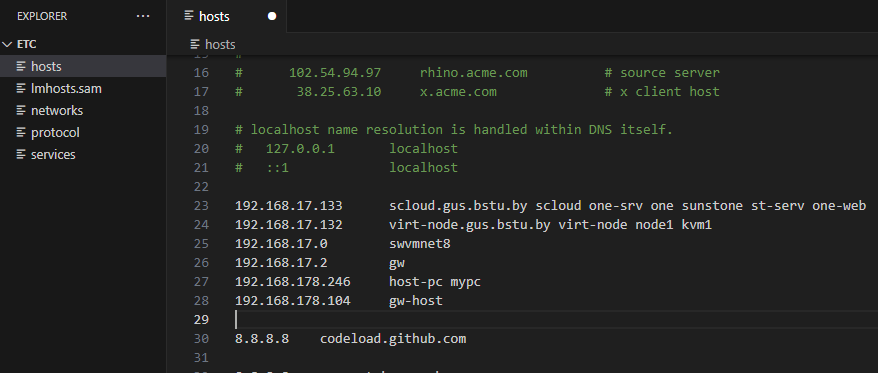
**Копирование файла /etc/hosts на хозяйскую машину**.

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).



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.

**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.**