**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:

$ sudo systemctl set-default multi-user.target

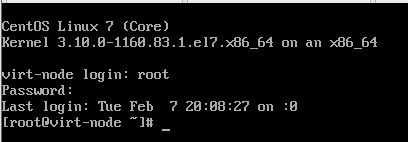
проверяем:

$ 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.

**1.2.1 Настройка ВМ, работающих под ОС CentOS 7.**

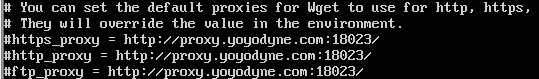
Примечание. При выполнении этого пункта уточните адрес прокси сервера у преподавателя.

1) Описать прокси сервер в настройках wget:

- Открыть в редакторе файл /etc/wgetrc

# nano /etc/wgetrc

- включить в этот файл посте строк:



следующие строки:

https\_proxy = <http://172.16.192.254:3128/>

http\_proxy = <http://172.16.192.254:3128/>

ftp\_proxy = <http://172.16.192.254:3128/>

use\_proxy = on

Сохранить файл /etc/wgetrc с внесенными изменениями.

2) Настроить работу yum с репозиториями, через прокси:

- открыть файл с именем **/etc/yum.conf** в редакторе nano:

# nano /etc/yum.conf

- внести в этот файл следующие строки:

proxy=http://172.16.192.254:3128

Сохранить файл /etc/yum.conf

3) Установить переменную окружения пользователя http\_proxy:

# export http\_proxy=http://172.16.192.254:3128

Проверить результат выполнения последней команды можно так:

# env | grep http\_proxy

4) Проверить список репозиториев

# yum repolist

5) Обновить информацию о пакетах репозиториев

# yum update

**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 |  | Сервер OpenNebula |
| 2 | **sunstone**  st-serv  one-web |  | Web-сервер Sunstone управления облаком |
| 3 | **virt\_node**  virt-node1  node1  kvm1 |  | Сервер виртуализации |
| 4 | **swvmnet8** |  | Виртуальный коммутатор VmNet8 |
| 5 | **gw** |  | Шлюз виртуальной сети облака |
| 6 | dns-srv |  | Сервер DNS |
| 7 | host-pc  mypc |  | Хозяйская машина |
| 8 | **gw-host** |  | 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:

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

# Local Addresses a components of the OpenNebula Cloud

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

st-serv one-web

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

192.168.15.1 swvmnet8

192.168.15.2 gw

192.168.100.200 host-pc mypc

192.168.100.1 gw-host

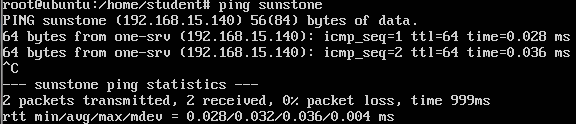
Примечение. В качестве разделителя имен могут использоваться следующие знаки:

- “ “ (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

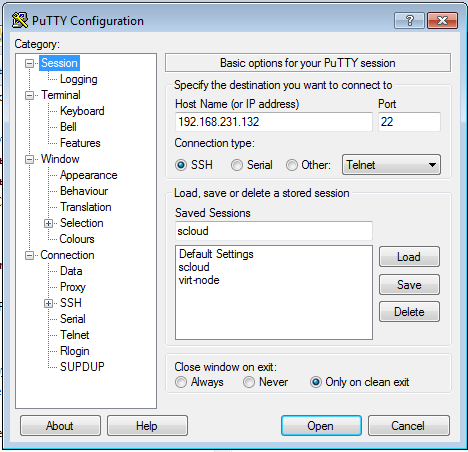
**1.4.1 Знакомство со средствами удаленного администрирования узлов сетевой инфраструктуры облаков.**

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**

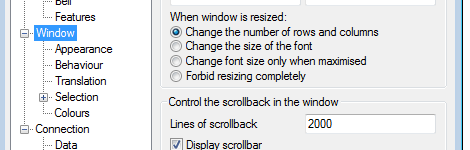
1) Всегда создавайте сохраненные сессии для работы с узлами требующими частых подключений:



Для этого служат кнопки Load и Save.

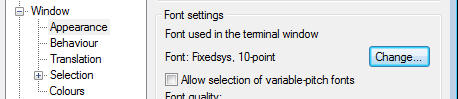
2) Настройки сессий для корректной работы с Midnight Commander:

**Window**

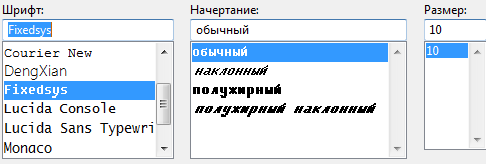


Установите размер буфера прокрутки экрана 20000 и более (макс. 32000)

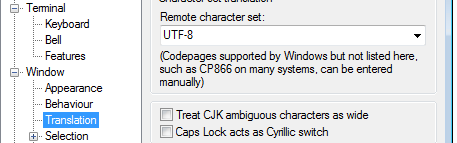
**Appearance**



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

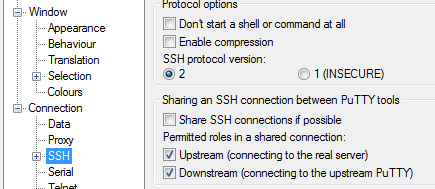


**Translation**



Выберите кодировку UTF-8

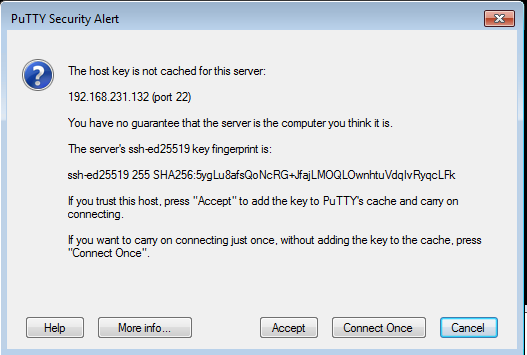
**SSH**



Выберите версию SSH 2

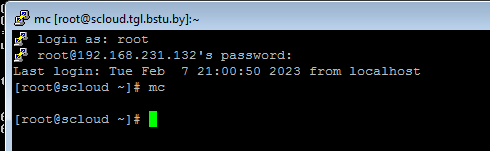
3) Согласование ключей

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

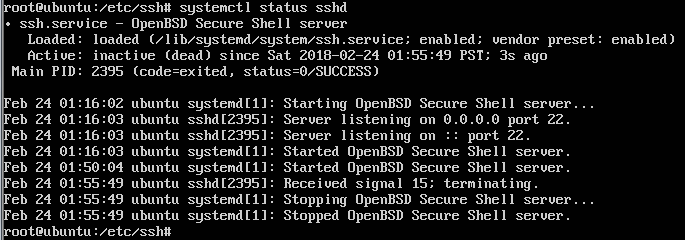
Ответ на эту команду должен быть следующим:



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

# systemctl restart sshd

Если же ответ на команду systemctl status sshd будет таким:



То службу sshd надо запустить с помощью команды:

# systemctl start sshd

3) Проверить работу служб SSHD на обоих узлах:

На управляющем выполнить подключение к самому себе:

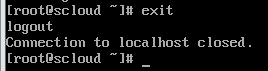
# ssh localhost



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.

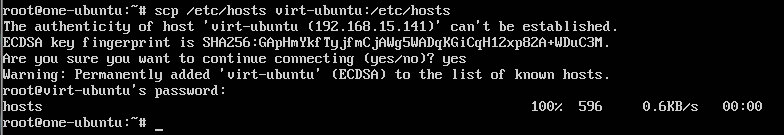
**1.4.3 Копирование файла /etc/hosts на рабочий узел и хозяйскую машину.**

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.

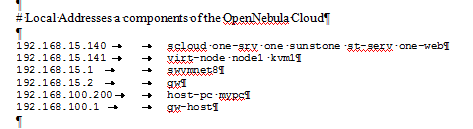
На машине scloud выполнить команду:

# 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).

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

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

1. Установить WinSCP на хозяйскую машину.
2. В окне, которое откроется после запуска WinSCP на хозяйской машине 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: 192.168.15.140 (адрес узла на котором имеется

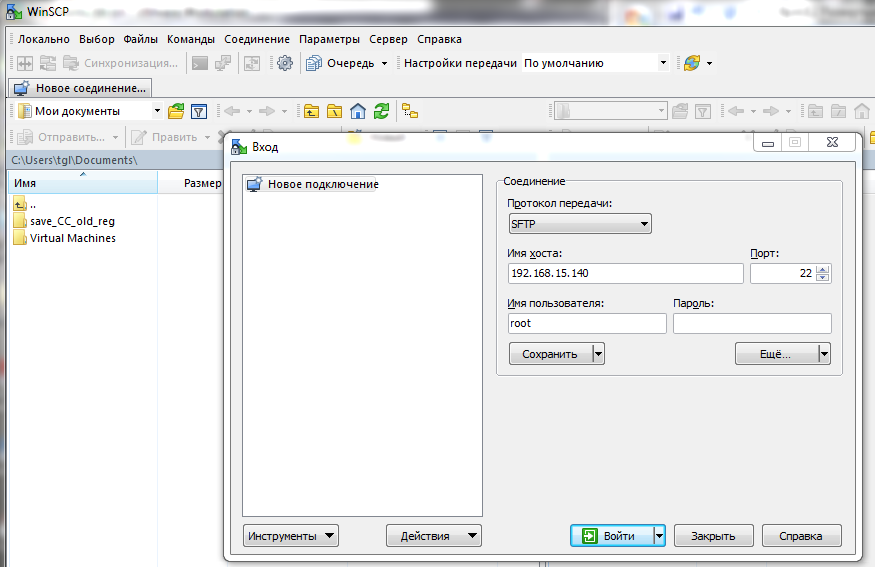
требуемый файл;

- порт: 22 (ssh);

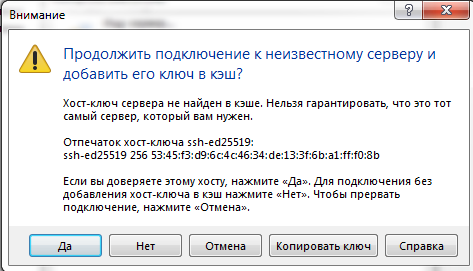
- имя пользователя: root

- пароль: оставить пустым.

c) Нажать кнопку «Войти»

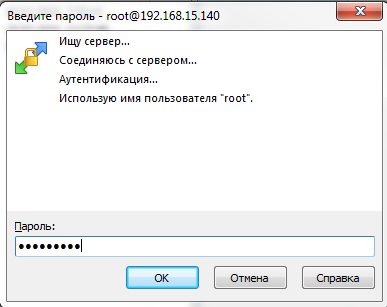


1. Откроется окно приема ключа.



Нажать «Да»

1. Откроется окно ввода пароля



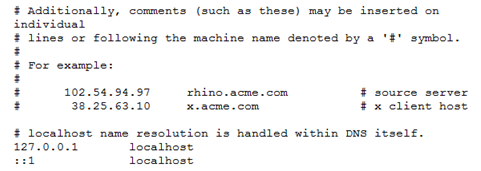
После ввода пароля нажать ОК. Если аутентификация на сервере scloud будет пройдена успешно, то откроется основное окно WinSCP имеющее вид схожий с TotalComander.

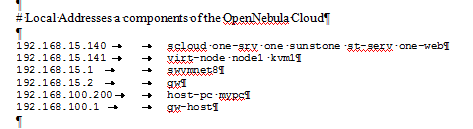
f) Далее нужно выполнить:

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

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

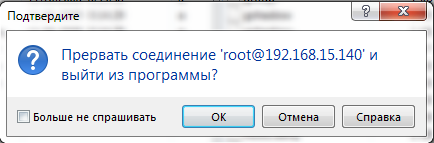
- скопировать в локальный файл hosts записи об именах облачных машин из экспортированного файла hosts и раскомментировать записи localhost;



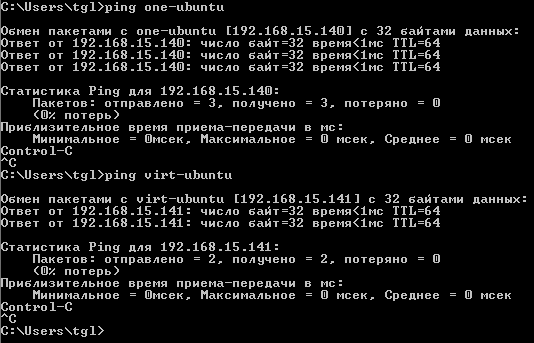


- сохраните с изменениями локальный файл hоsts в каталоге c:\Windows\System32\drivers\etc\ под именем hosts (без расширения!);

- закройте программу WinSCP, подтвердив разрыв соединения по SSH с узлом scloud;



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.

**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.**