Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Лабораторная работа № 3

Студент: Гурина К. С.

ФИТ 4 курс 4 группа

Минск 2024

**Облачные технологии**

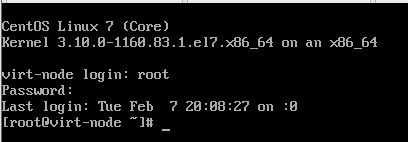
**Подготовка виртуальных машин к развертыванию облака OpenNebula**

**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



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.**

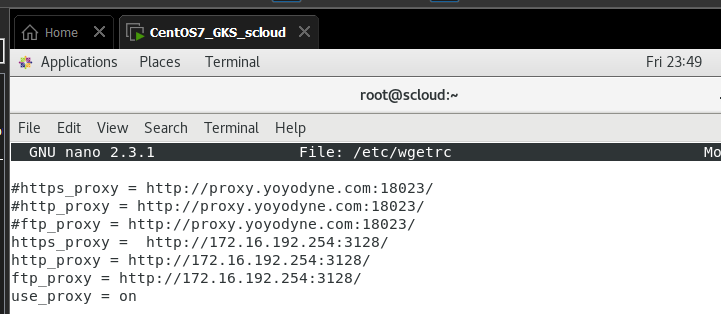
Примечание. При выполнении этого пункта уточните адрес прокси сервера у преподавателя.

1) Описать прокси сервер в настройках wget:

- Открыть в редакторе файл /etc/wgetrc

# nano /etc/wgetrc

- включить в этот файл посте строк:



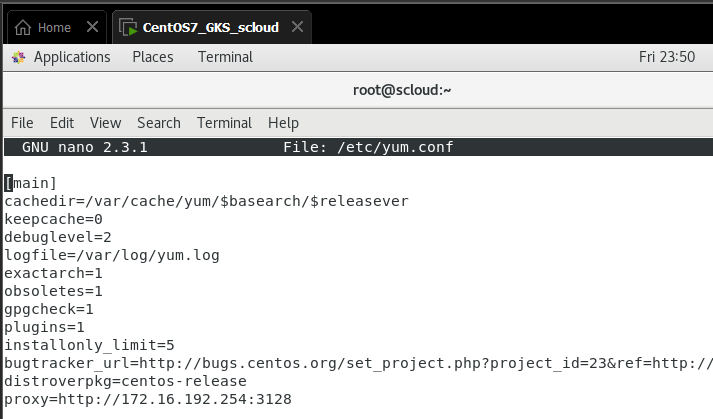
2) Настроить работу yum с репозиториями, через прокси:

- 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



**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 | 192.168.88.132 | Сервер OpenNebula |
| 2 | **sunstone**  st-serv  one-web | 192.168.88.132 | Web-сервер Sunstone управления облаком |
| 3 | **virt\_node**  virt-node1  node1  kvm1 | 192.168.88.128 | Сервер виртуализации |
| 4 | **swvmnet8** | 192.168.88.1 | Виртуальный коммутатор VmNet8 |
| 5 | **gw** | 192.168.88.2 | Шлюз виртуальной сети облака |
| 6 | dns-srv | 192.168.88.2 | Сервер DNS |
| 7 | host-pc  mypc | 192.168.31.252 | Хозяйская машина |
| 8 | **gw-host** | 192.168.31.1 | 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:

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

# Local Addresses a components of the OpenNebula Cloud

192.168.88.132 scloud.gks.bstu.by scloud one-srv one sunstone st-serv one-web

192.168.88.128 virt-node.gks.bstu.by virt-node node1 kvm1

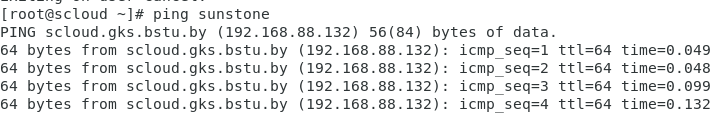
192.168.88.1 swvmnet8

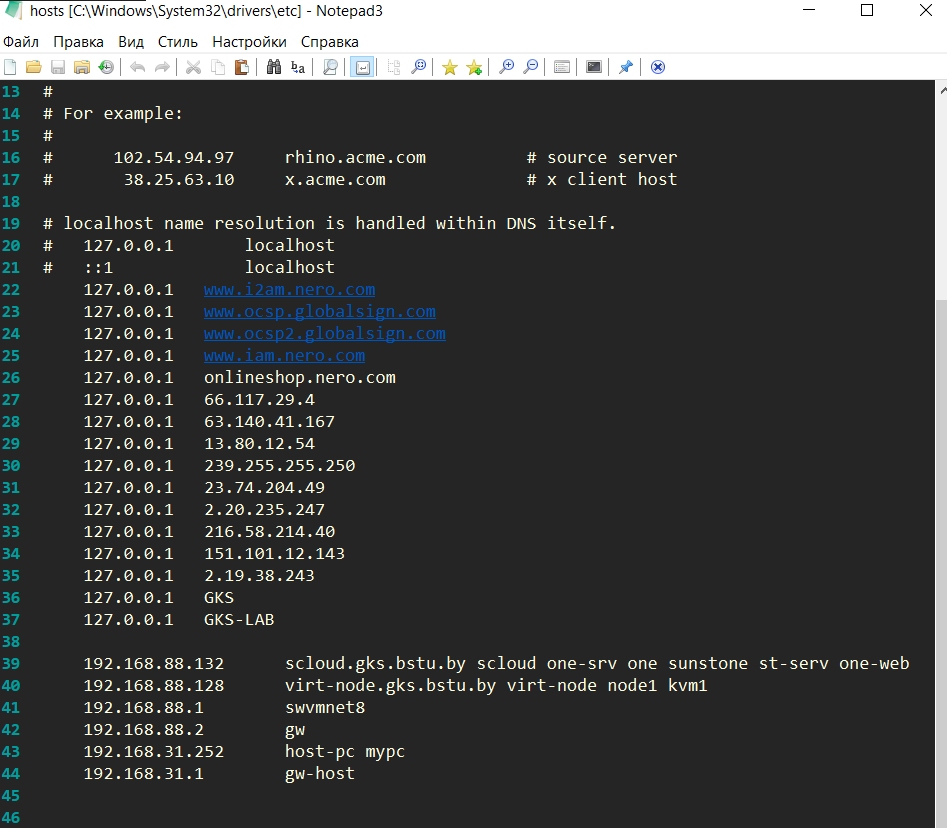
192.168.88.2 gw

192.168.31.252 host-pc mypc

192.168.31.1 gw-host

Проверить правильность назначения имен можно с помощью команды ping:



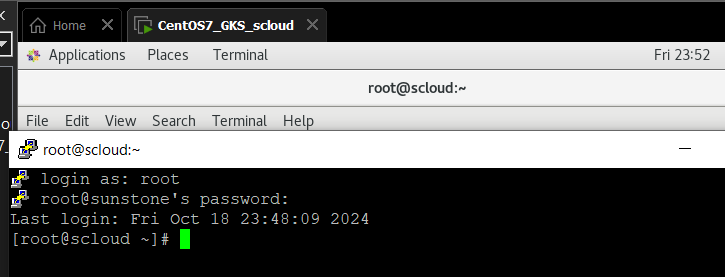


**1.4. Настроить работу службы сервер SSH на главном и рабочем узлах предназначенных для развертывания ОН**

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

Для принятия ключей кликните Accept.

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



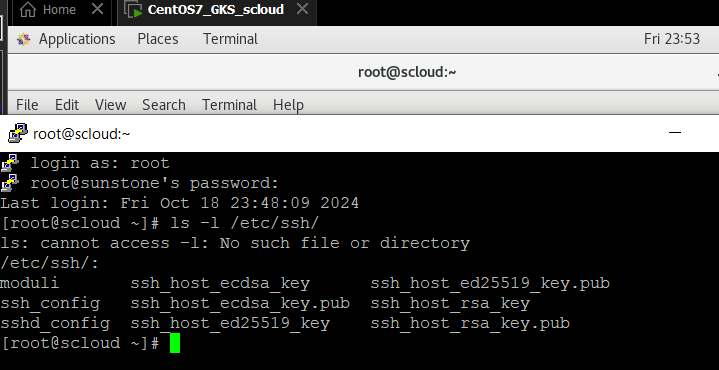
Теперь можно с ВМ scloud имея возможность копировать текст из окна терминала.

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

1) Просмотреть содержимое папки /etc/ssh:

# ls –l /etc/ssh/

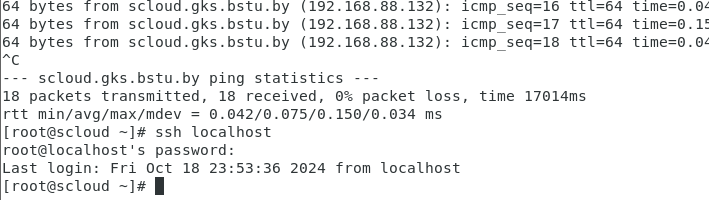
Если в этом каталоге есть конфигурационный файла sshd\_config



Проверить работу служб SSHD на обоих узлах:

На управляющем выполнить подключение к самому себе:

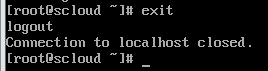
# ssh localhost



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:

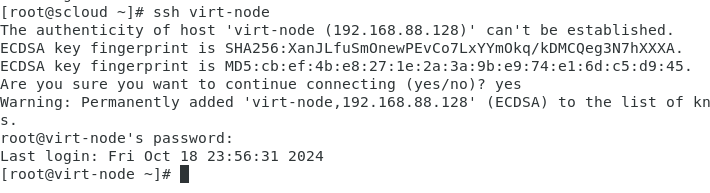
# exit



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

С узла scloud:

# ssh 192.168.88.128



**Ответы на контрольные вопросы**

**Для чего предназначена служба Telnet?**  
Telnet предназначен для удаленного доступа к устройствам и серверам, позволяя пользователям управлять ими через текстовый интерфейс.

**Какой протокол транспортного уровня использует служба Telnet?**  
Telnet использует протокол TCP (Transmission Control Protocol).

**Какой порт TCP является стандартным для Telnet?**  
Стандартный порт TCP для Telnet — 23.

**В чем состоит основная опасность использования Telnet?**  
Основная опасность заключается в том, что Telnet передает данные, включая логины и пароли, в открытом виде, что делает их уязвимыми для перехвата.

**Объясните, почему Telnet широко используется администраторами сетей для диагностики работы других информационных служб Интернет?**  
Telnet позволяет администраторам выполнять текстовые команды на удаленных устройствах, что облегчает диагностику и управление сетевыми службами, особенно когда другие методы доступа недоступны.

**Для чего предназначена служба SSH?**  
SSH (Secure Shell) предназначен для безопасного удаленного доступа к устройствам и серверам, обеспечивая шифрование всех передаваемых данных.

**Какой протокол транспортного уровня использует служба SSH?**  
SSH также использует протокол TCP.

**Какой порт TCP является стандартным для SSH?**  
Стандартный порт TCP для SSH — 22.