Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Дисциплина «Облачные системы»

**Отчёт по лабораторной работе №3**

Подготовка виртуальных машин к развертыванию облака OpenNebula

Студент: Глухова Д.В.

ФИТ 4 курс 2 группа

Преподаватель: Бернацкий П.В.

**Содержание**

[**1 Подготовка виртуальных машин к развертыванию облака OpenNebula** 3](#_Toc209252410)

[**2 Работа со службой Telnet** 5](#_Toc209252411)

[**3 Работа со службой SSH.** 8](#_Toc209252412)

[**4 Настроить работу службы сервер SSH на главном и рабочем узлах предназначенных для развертывания ОН** 9](#_Toc209252413)

[**5 Ответы на вопросы** 15](#_Toc209252414)

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

Необходимо отключить запуск X-ов при старте системы. Используем команду sudo systemctl set-default multi-user.target. Результат представлен на рисунке 1.1.

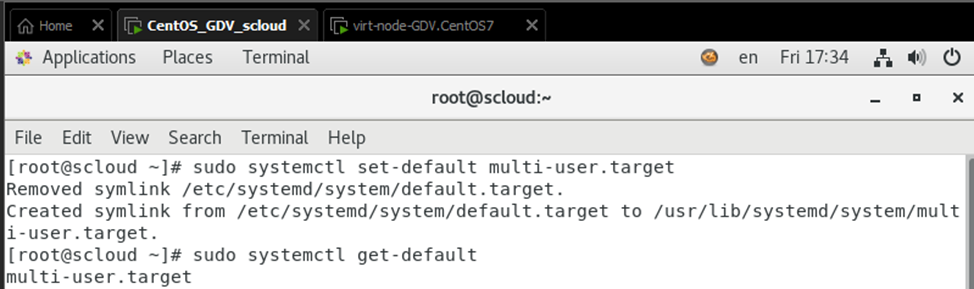


Рисунок 1.1 – Отключение запуск X-ов при старте системы на первой ВМ

На второй ВМ аналогично вводим ту же команду.

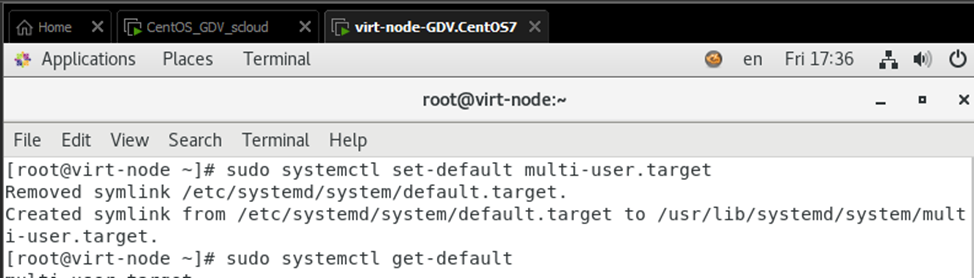


Рисунок 1.2 – Отключение запуск X-ов при старте системы на второй ВМ

Далее при запуске машин не будет GUI, работа происходит только с командной строкой.



Рисунок 1.3 – Проверка на первой ВМ

На второй машине то же самое.

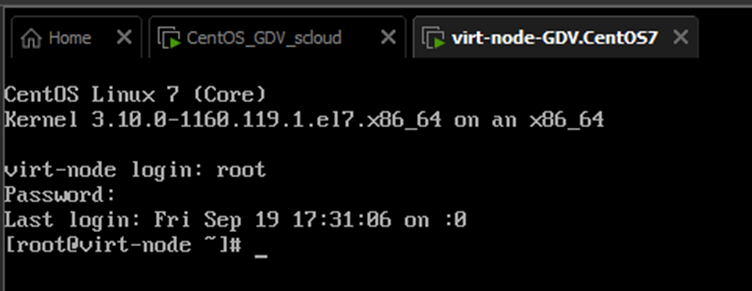


Рисунок 1.4 – Проверка на второй ВМ

Далее заполним таблицу 1.1 имен и IP адресов ВМ, входящих в состав облака. Данные для таблицы можно взять из предыдущей работы.

Таблица 1.1. Таблица имен и IP адресов ВМ, входящих в состав облака.

|  |  |  |  |
| --- | --- | --- | --- |
| № п.п | Имя узла\* | IP адрес узла\*\* | Назначение узла |
| 1 | **scloud**  one-serv | 192.168.216.128 | Сервер OpenNebula |
| 2 | **sunstone**  st-serv  one-web | 192.168.216.128 | Web-сервер Sunstone управления облаком |
| 3 | **virt\_node**  virt-node1  node1  kvm1 | 192.168.216.129 | Сервер виртуализации |
| 4 | **swvmnet8** | 192.168.216.1 | Виртуальный коммутатор VmNet8 |
| 5 | **gw** | 192.168.216.2 | Шлюз виртуальной сети облака |
| 6 | dns-srv | 192.168.216.2 | Сервер DNS |
| 7 | host-pc  mypc | 192.168.0.167 | Хозяйская машина |
| 8 | **gw-host** | 192.168.0.1 | Шлюз хозяйской машины |

На управляющем узле scloud откроем файл /etc/hosts. Внесем в него следующие записи, после записей 127.0.0.1, но до адресов IPv6.

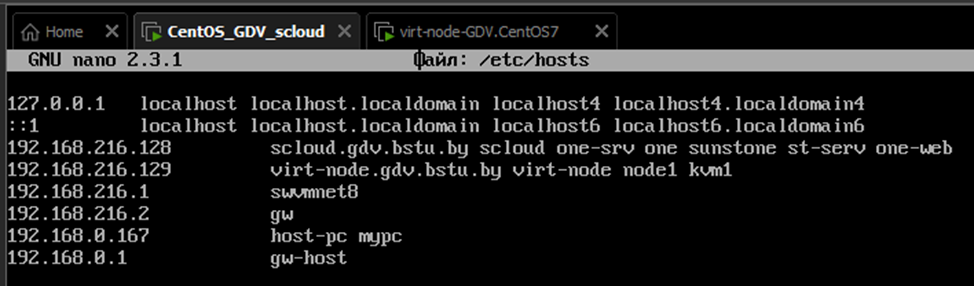


Рисунок 1.5 – Установка имен узлов облака в файл /etc/hosts на первой ВМ

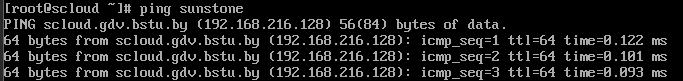


Рисунок 1.6 – Проверка правильности назначения имен

# **2 Работа со службой Telnet**

Для начала работы со службой необходимо включить компонент Клиент Telnet.

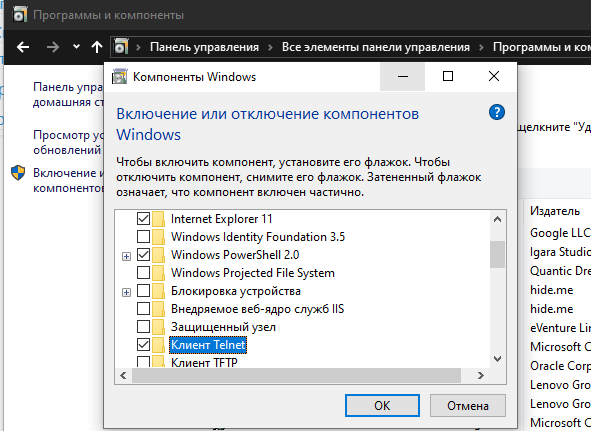


Рисунок 2.1 – Установка компонента Клиент Telnet

С помощью команды help можно получить справку по командам доступным в командном режиме. Просмотреть рабочие параметры можно с помощью команды display. Изменить значение комбинации можно с помощью set escape x.

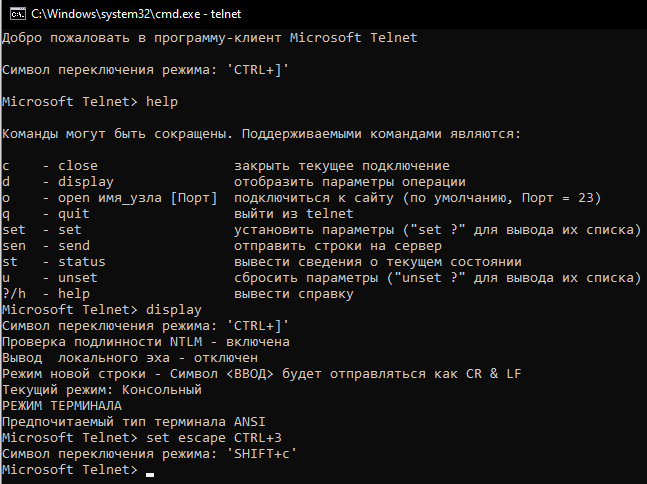


Рисунок 2.2 – Команда help, переключение режима

Для подключения к серверу используется open <сервер>.



Рисунок 2.3 – Подключение к серверу Telnet

После подключения к серверу видим следующее окно, представленное на рисунке.

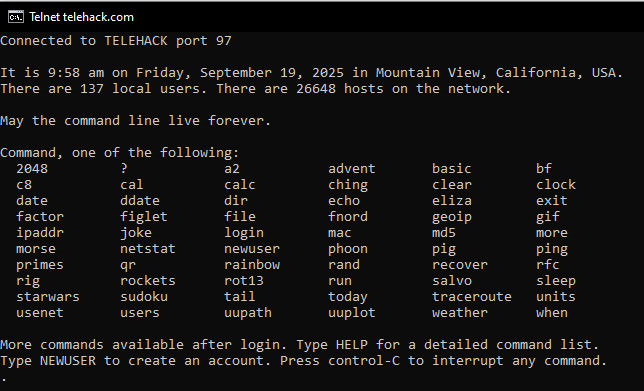


Рисунок 2.4 – Вывод после подключения

При запуске программы PuTTY, отроется окно конфигурирования программы.

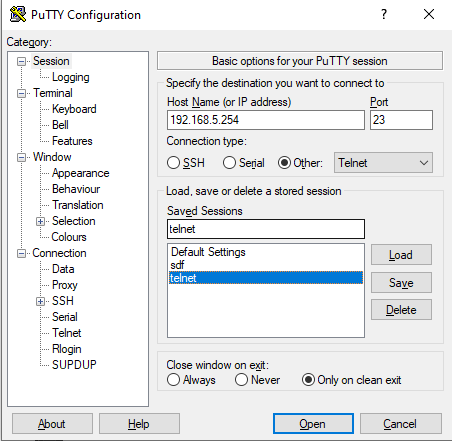


Рисунок 2.5 – Создание сохраненных сессий

При подключении к серверу необходимо будет создать пользователя для дальнейшей авторизации.

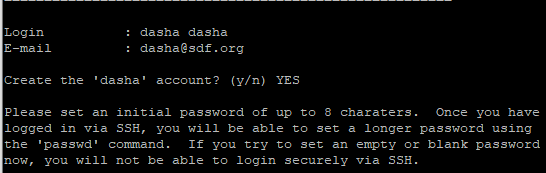


Рисунок 2.6 – Создание пользователя

Выполнение команд cd, ls, pwd, top представлены на рисунке 2.7 и 2.8.

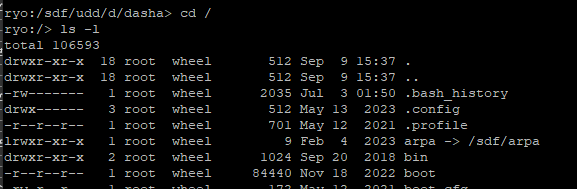


Рисунок 2.7 – Переход в корневой каталог и просмотр содержимого

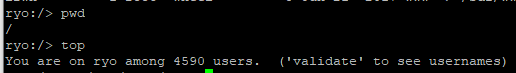


Рисунок 2.8 – Вывод имени текущего каталога

Для создания файла используется команда touch.

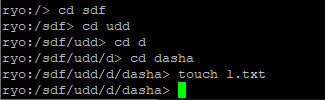


Рисунок 2.9 – Переход в каталог и создание файла

Для изменения файла используется nano.

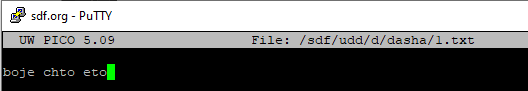


Рисунок 2.10 – Содержимое файла

Для отправки на почту используется mail.

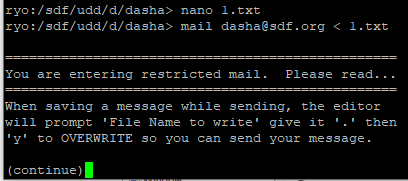


Рисунок 2.11 – Отправка содержимого на почту

Для отключения от сервера используем команду exit и видим следующее окно:

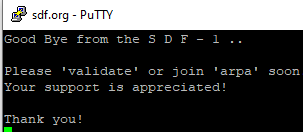


Рисунок 2.12 – Отключение от сервера

# **3 Работа со службой SSH.**

При первом подключении используя SSH появится окно о том, что для сервера присутствуют ключи шифрования.

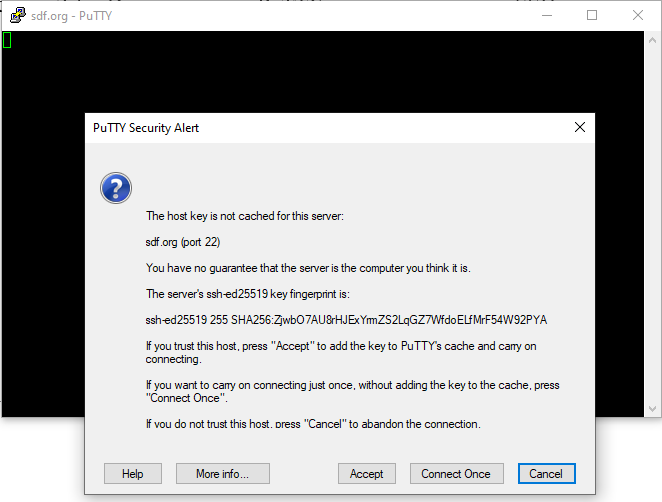


Рисунок 3.1 – Соглашение на использование предлагаемых ключей

После входа в систему выполним следующие команды: pwd, whoami, who. Команда deco запускает командную оболочку, которая позволяет перемещаться по файловой системе не зная команд OS UNIX.

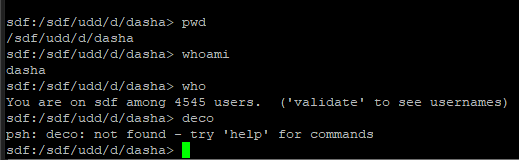


Рисунок 3.2 – Результат выполнения команд

Заключение: в ходе работы со службой SSH с использованием программы PuTTY было выполнено подключение к учебному серверу, проведена аутентификация с вводом логина и пароля, а также освоены базовые команды ОС UNIX.

# **4 Настроить работу службы сервер SSH на главном и рабочем узлах предназначенных для развертывания ОН**

Для комфортной работы с PuTTY, рекомендуется выполнить следующие настройки:

Изображение выглядит как текст, снимок экрана, Шрифт, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 4.1 – Установка размера буфера прокрутки экрана 20000

Изображение выглядит как текст, Шрифт, число, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 4.2 – Appearance

Изображение выглядит как текст, снимок экрана, дисплей, число

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 4.3 – Установка шрифта

Изображение выглядит как текст, Шрифт, число, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 4.4 – Appearance

Изображение выглядит как текст, снимок экрана, дисплей, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 4.5 – Translation кодировка UTF-8

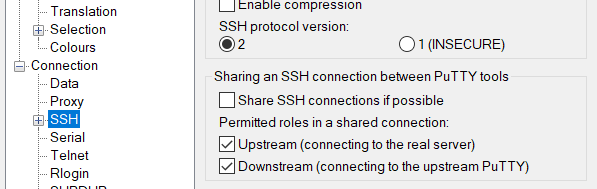


Рисунок 4.6 – Версия SSH 2

Для подключения к ВМ создаем новое подключение и вводим данные пользователя.

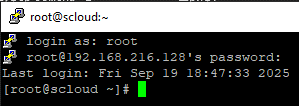


Рисунок 4.7 – Подключение к ВМ через PuTTY

Для просмотра содержимого папки используем команду ls <папка>.

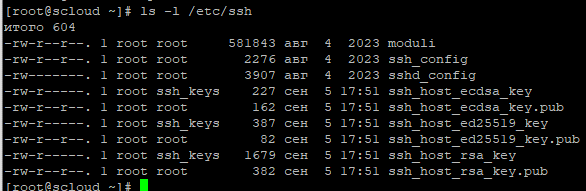


Рисунок 4.8 – Просмотр конфигурационного файла sshd\_config

Для того чтобы отредактировать файл используем nano. Раскомментируем строки PermitRootLogin и PasswordAuthentication.

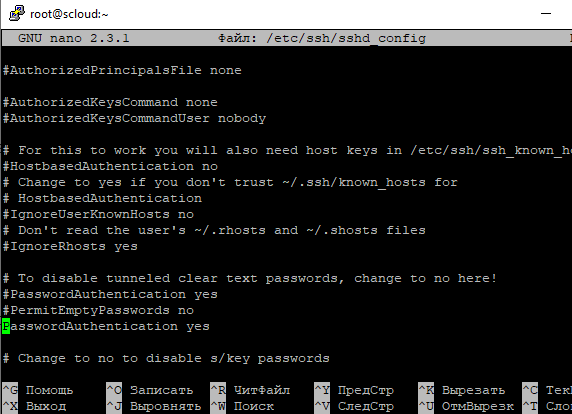


Рисунок 4.9 – Настройка сервера SSHD

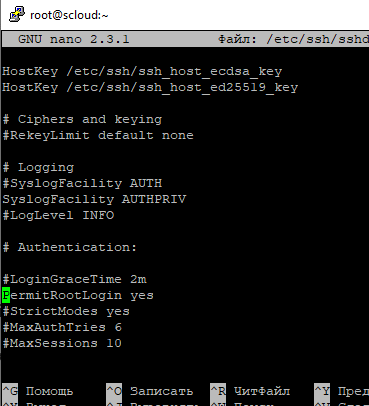


Рисунок 4.5 – Настройка сервера SSHd

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.

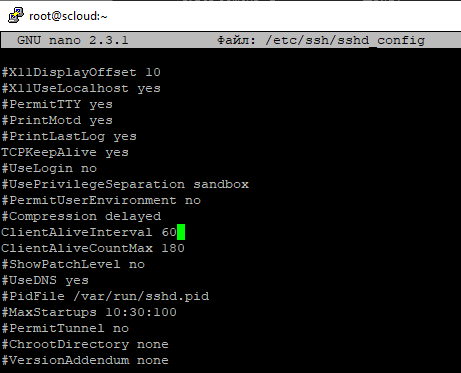


Рисунок 4.6 – Настройка сервера SSHd

Убедимся, что ОС использует systemd.



Рисунок 4.7 – ОС использует system

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

Проверим запущена ли служба сервера SSHD, для этого используем команду systemctl status sshd. Получаем положительный ответ.

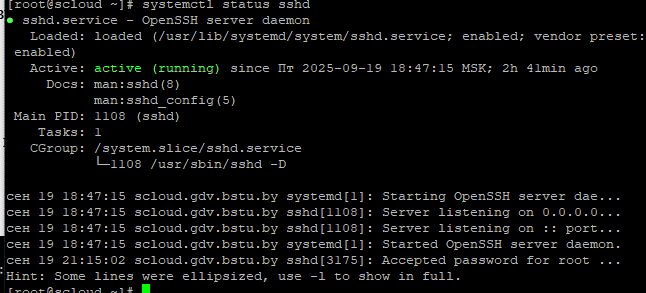


Рисунок 4.8 – Запущена ли служба сервера SSHD

Для перезапуска службы используем systemctl restart sshd, затем вновь проверяем статус службы.

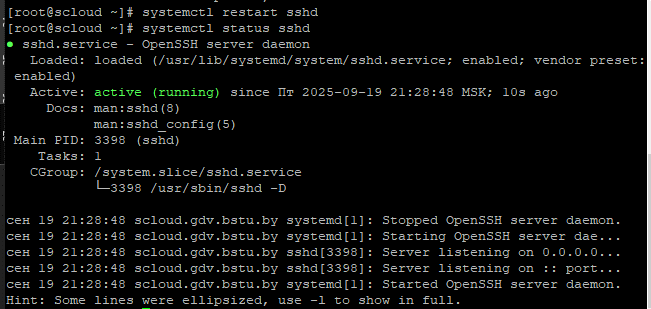


Рисунок 4.9 – Перезапуск службы

Чтобы проверить работу служб SSHD, на обоих узлах выполним подключение к самому себе. Используем для этого ssh localhost.

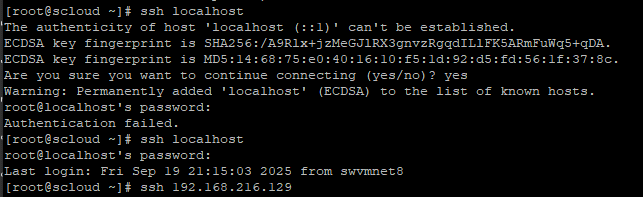


Рисунок 4.10 – Проверка работы службы SSHD на первой ВМ

На второй ВМ также используем ssh localhost.

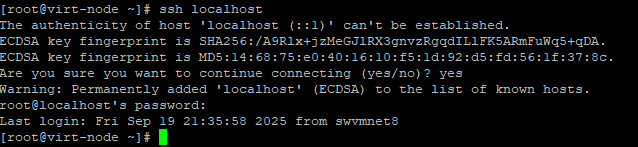


Рисунок 4.11 – Проверка работы службы SSHD на второй ВМ

Далее проверим возможность подключения узлов друг к другу в обоих направлениях. Для этого используем ssh <ip>.

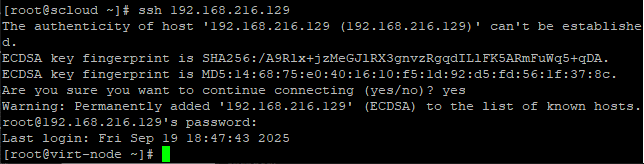


Рисунок 4.12 – Проверка работы службы SSHD на первой ВМ

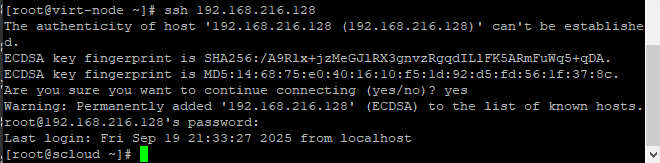


Рисунок 4.13 – Проверка работы службы SSHD на второй ВМ

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

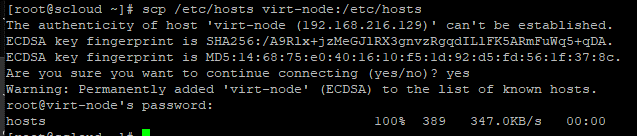


Рисунок 4.14 – Копирование файла /etc/hosts на первой ВМ

Для просмотра правильности выполнения используем cat.

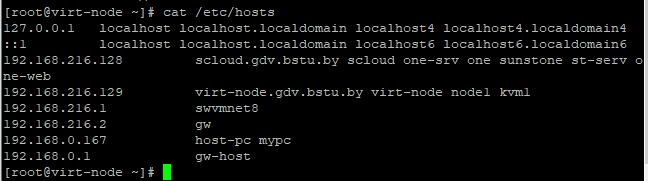


Рисунок 4.15 – Просмотр файла /etc/hosts на второй ВМ

Для копирования файла на хозяйскую машину просто добавим в файл новые записи вручную.

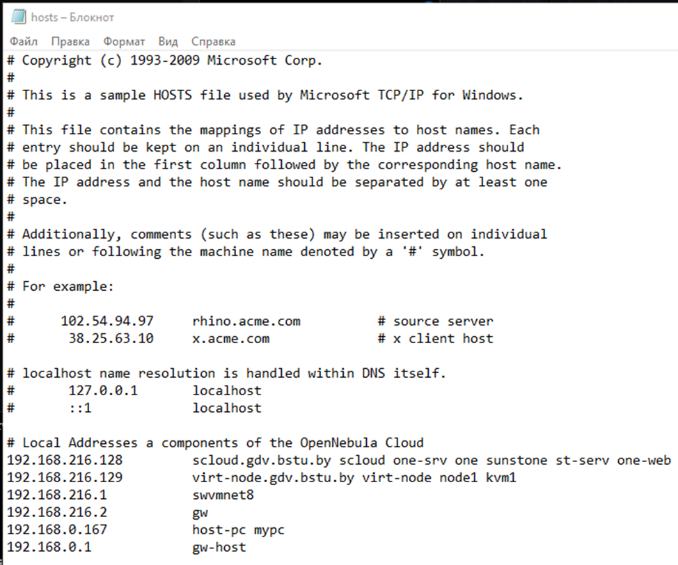


Рисунок 4.16 – Установка имен узлов облака в файл /etc/hosts на хосте

Для проверки правильности выполнения также используем команду ping.

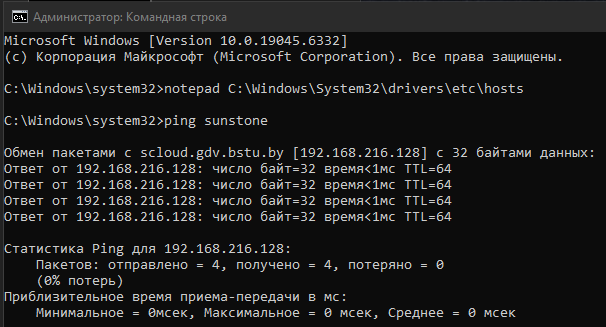


Рисунок 4.17 – Проверка

**5 Ответы на вопросы**

1. Для чего предназначена служба Telnet? Telnet предназначен для удаленного доступа к компьютерам и серверам через сеть, позволяя пользователям управлять удаленными системами через командную строку.
2. Какой протокол транспортного уровня использует служба Telnet? Telnet использует протокол TCP (Transmission Control Protocol).
3. Какой порт TCP является стандартным для Telnet? Стандартный порт TCP для Telnet – 23.
4. В чем состоит основная опасность использования Telnet? Основная опасность использования Telnet заключается в отсутствии шифрования данных, что делает его уязвимым для перехвата и анализа злоумышленниками.
5. Объясните, почему Telnet широко используется администраторами сетей для диагностики работы других информационных служб Интернет? Telnet позволяет администраторам сетей быстро и легко подключаться к удаленным системам для выполнения диагностики и устранения неполадок, благодаря своей простоте и доступности.
6. Для чего предназначена служба SSH? SSH (Secure Shell) предназначен для безопасного удаленного доступа и управления компьютерами и серверами, обеспечивая шифрование данных и аутентификацию пользователей.
7. Какой протокол транспортного уровня использует служба SSH? SSH использует протокол TCP.
8. Какой порт TCP является стандартным для SSH? Стандартный порт TCP для SSH – 22.
9. Кратко расскажите о возможностях программы PuTTY. PuTTY – это бесплатный клиент для удалённого доступа через протоколы SSH, Telnet и другие. Позволяет подключаться к серверам и выполнять команды на удалённой машине через терминал.
10. Каково назначение и основные функции программ deco и Midnight Commander (mc)? Deco – это текстовый редактор для работы в консоли. Основные функции: редактирование, поиск, замена текста, работа с файлами. Midnight Commander (mc) – это консольный файловый менеджер с двухпанельным интерфейсом, который позволяет легко выполнять операции с файлами (копирование, перемещение, удаление) и просматривать их содержимое.
11. Горячие клавиши в deco и mc:

* Выделение файлов и каталогов: Insert
* Копирование файлов и каталогов: F5
* Перемещение файлов и каталогов: F6
* Удаление файлов и каталогов: F8
* Создание каталогов: F7
* Редактирование файлов: F4
* Справка по функциям программы: F1
* Поиск подстрок в файлах: F7 (mc), Ctrl + W (deco)