University: [ITMO University](https://itmo.ru/ru/)

Faculty: [FICT](https://fict.itmo.ru/)

Course: [Network programming](https://github.com/itmo-ict-faculty/network-programming)

Year: 2022

Group: K34212

Автор: Сорокина Ирина Игоревна

Lab: Lab1

Date of create: 20.09.2022

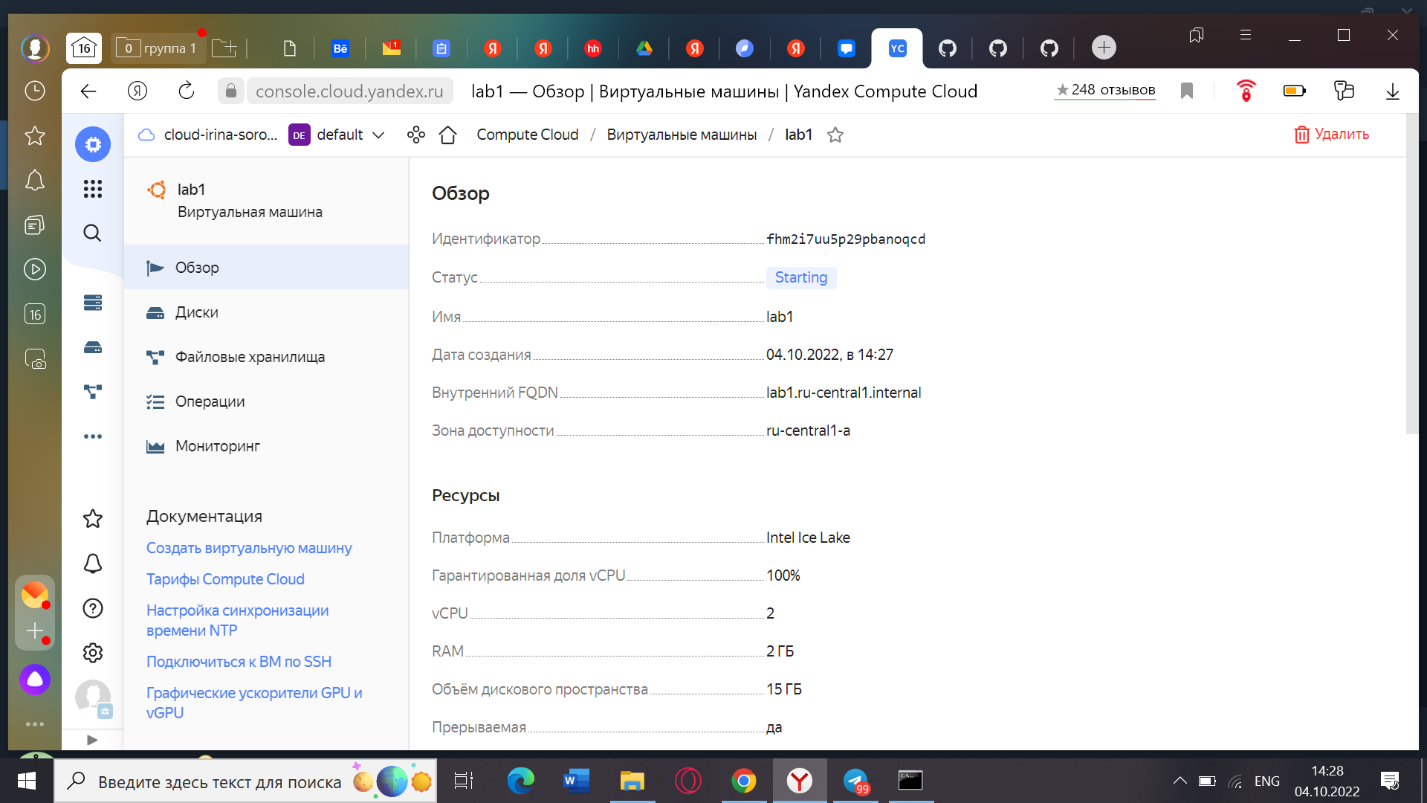
Date of finished:

Тема работы: Установка CHR и Ansible, настройка VPN

Цель работы: развертывание виртуальной машины с установленной системой контроля конфигураций Ansible, установка CHR в VirtualBox, установка VPN туннеля между машиной Ubuntu и RouterOS.

Ход работы:

1. Развернула ВМ «Ubuntu» на платформе «Яндекс Облако».



*Информация о ВМ*

2. Установка системы контроля конфигураций «Ansible» на ВМ.

* Обновила ВМ «Ubuntu» с помощью команд:

sudo apt update

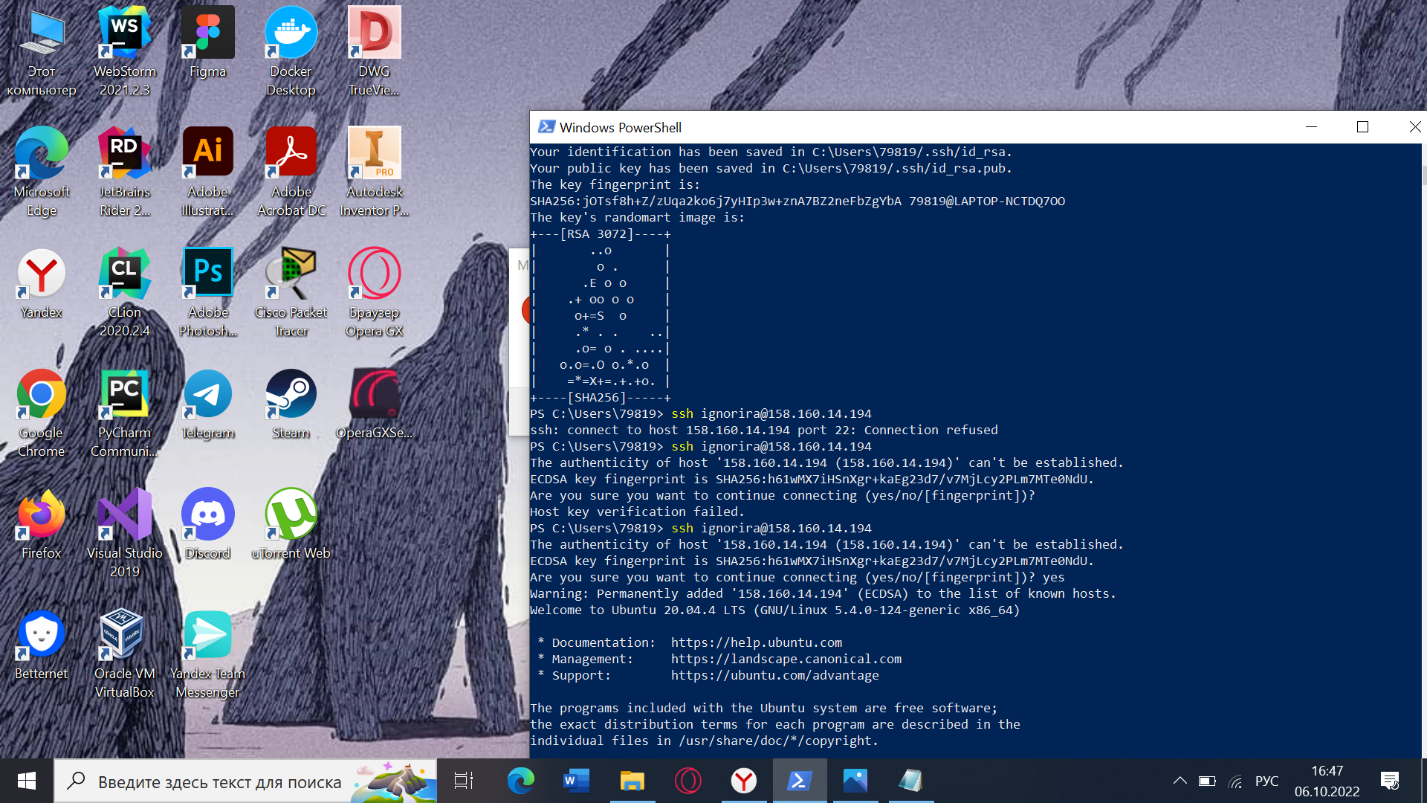
sudo apt upgrade

* Установила python3 и Ansible

sudo apt install python3-pip

sudo pip3 install ansible

* Подключилась к виртуальной машине в Яндекс.Облаке по ssh.

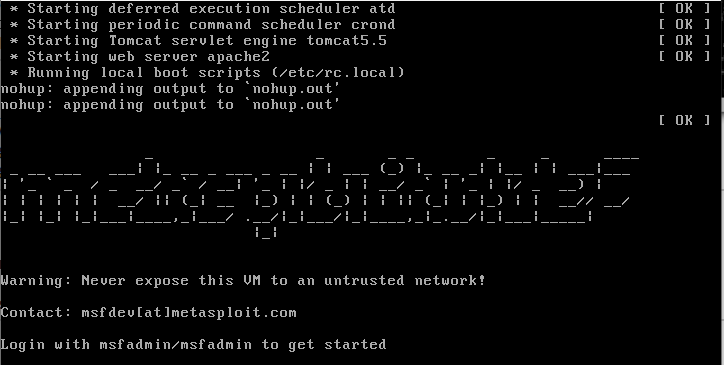


3. Установка CHR на VirtualBox

* Загрузила VDI файл с [https://mikrotik.com](https://mikrotik.com/)
* Установила CHR на VirtualBox с помощью загруженного файла (после загрузки в настройках VirtualBox отключила загрузочный диск вручную).

### 4. Создание Wireguard сервера на машине Ubuntu и настройка Wireguard клиента на RouterOS.

* Устанавила Wireguard на удалённую машину (sudo apt install wireguard), прописала в нём в файл условий интерфейса. Создала пару ключей.
* Затем начала работу с MikroTik. Поставила эмулятор графического интерфейса, умеющий запускать exe файлы. Подключилась к виртуальной машине MikroTik.



* Поскольку в качестве VPN был выбран WireGuard, и установлен MikroTik последней версии, зашла в настройки Wireguard и создала там новый интерфейс. Заполнила строки:
* MTU оставляем 1420;
* ListenPort узнаём командой вывода файла /etc/wireguard/wg0.conf на сервере (13231);
* ключи сгененрированы автоматически.

Изображение выглядит как текст

Автоматически созданное описание

* Перешла во вторую вкладку, там создала Peer, указала там:
* созданный интерфейс wireguard1
* публичный ключ сервера;
* публичный IP сервера;
* указанный ранее порт;
* сеть адресов, по которым будет идти подключение.

Изображение выглядит как текст

Автоматически созданное описание

* В настройке IP - Addresses указала выбранную сеть и созданный интерфейс.

Изображение выглядит как текст

Автоматически созданное описание

* В настройке IP - Firewall создала Masquerade NAT. Он позволяет преобразовывать несколько IP-адресов в другой одиночный IP-адрес.

Изображение выглядит как текст

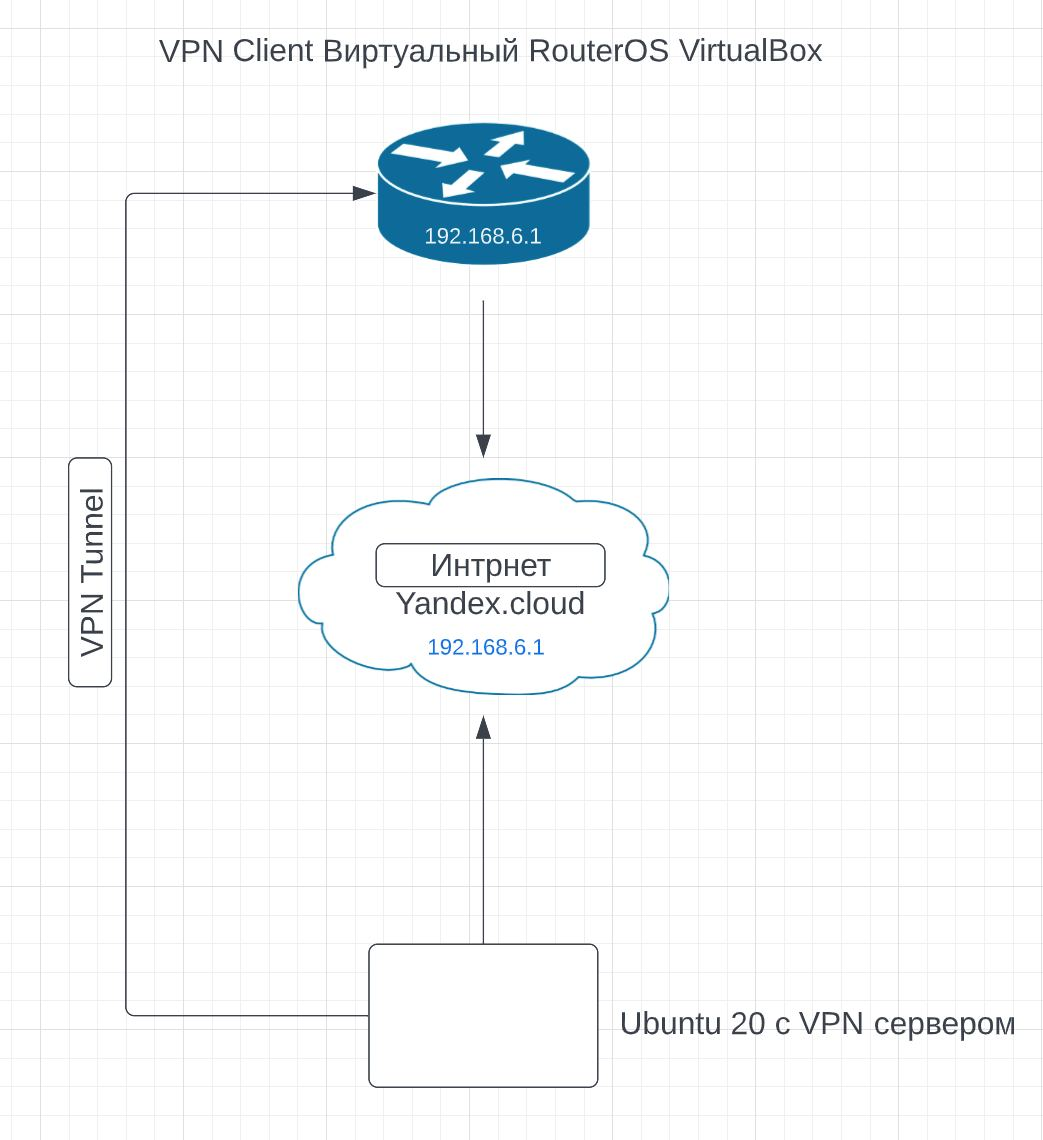
Автоматически созданное описание

* Запустила ping к ВМ по IP адресу 192.168.6.1 для проверки работоспособности.

Изображение выглядит как текст

Автоматически созданное описание

* В результате получаем связь по следующей схеме.



Вывод:

В ходе выполнения лабораторной работы мне удалось развернуть ВМ с установленной системой контроля конфигураций Ansible, установить CHR в VirtualBox, и пробросить VPN туннель между ВМ Ubuntu с ОС RouterOS и удаленной виртуальной машиной при помощи WireGuard.