**Документ памятка для системного администратора**.

Инфраструктура состоит из 2х серверов:

1. Сервер PKI и VPN
2. Сервер системы мониторинга Prometheus, включающий еще в себя alertmanager.

Если планируется разворот инфраструктуры в облаке Yandex Cloud\VK cloud\MTS cloud\Sber cloud и.т.п, то нужно настроить доступ по ключу ssh.

Для формирования ssh ключей используем команду:

ssh-keygen

На запрос о местоположении ключа оставлять все по умолчанию. При создании виртуального ПК на облачном провайдере, ключ указывается на этапе создания

При формировании посредством виртуализации на локальном хосте, либо же разворачивании системы на физический ПК, следует отключить опцию ssh сервера вход по паролю

PubkeyAuthentication yes

PermitRootLogin No

PasswordAuthentication No

Перезапускаем слубу ssh

sudo systemctl restart sshd

Проверяем корректное подключение по SSH. Далее обновляемся

Sudo apt update -y && sudo apt upgrade -y

И установим easy-rsa и openvpn

sudo apt install easy-rsa openvpn -y

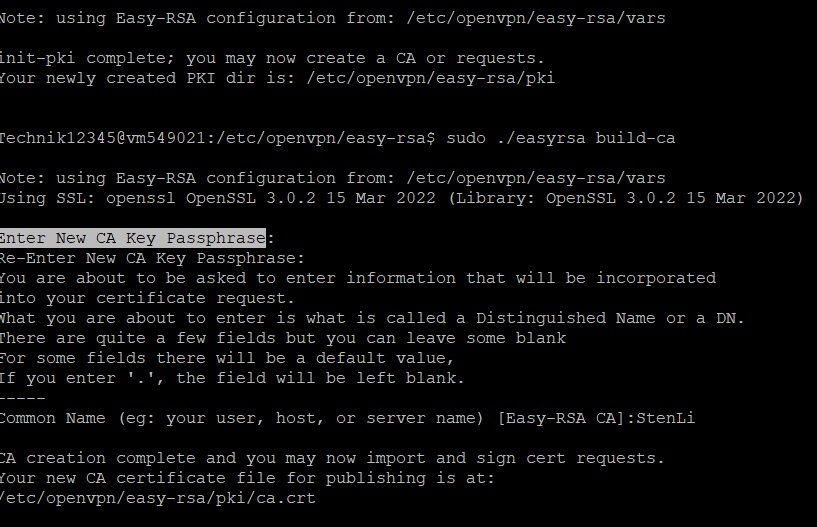
Для ускорения настройки использовать **easy-rsa\_0.1-1\_all.deb** и **openvpn\_0.1-1\_all.deb**, которые уже несут в себе необходимую конфигурацию

**sudo** **dpkg** **-i** easy-rsa\_0.1-1\_all.deb

**sudo** **dpkg** **-i** openvpn\_0.1-1\_all.deb

Ждем пока команды все отработают.

Внимание при работе команд PKI скрипт запросит пасс фразу (Enter New CA Key Passphrase) для формирования ключа удостоверяющего центра, вводим ее и запоминаем



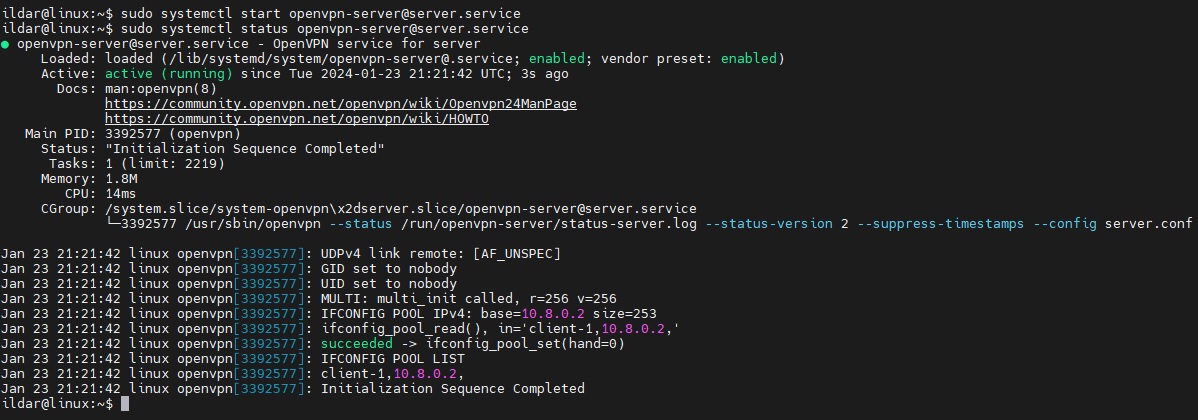
Также сформируется сертификат для ВПН сервера и секретный ключ. При подписи сертификата потребуется ввести passphrase, которую мы указывали ранее.

Далее запустим службу openvpn

sudo systemctl enable openvpn-server@server.service

sudo systemctl start openvpn-server@server.service

sudo systemctl status openvpn-server@server.service



В случаи неудачи смотрим лог который находится /var/log/openvpn/openvpn.log

Для настройки клиентской части VPN используйте dep пакет **client-req\_0.1-1\_all.deb,** вносящий необходимые настройки. Также для формирования клиентских конфигураций используйте скрипт **make\_client\_conf.sh.**

Клиент отправляет запрос на предоставление доступа по ВПН, посредством письма на email.

**ВАЖНО: Доступ к корпоративной сети посредством ВПН сотруднику следует выдавать только после письменного согласования его руководителя и руководителя службы безопасности.**

**Не раздавать доступы без необходимых согласований!!!**