**Руководство по развертыванию удостоверяющего центра**

1. Для удостоверяющего центра необходима машина с установленной любым удобным способом ОС Linux с внутренним IP-адресом 10.128.0.10 и именем **ca**. Данная машина не будет иметь прямой выход в сеть и будет находиться за NAT’ом. Подключение будет осуществляться через машину VPN и monitoring. Еще необходимо создать пару ssh-ключей и обменяться публичным ключом с каждой машиной (vpn, bkp1,bkp2, monitoring).
2. Создаем в домашней директории пользователя папку **artefacts**, куда копируем скрипты автоматизации и установочные пакеты.
3. Для развертывания СА- сервера необходимо запустить скрипт **caDeploy.sh** от имени суперпользователя.

Данный скрипт совершит следующие действия:

* Для начала установит часовой пояс по Москве и синхронизирует с ним время
* Обновит кеш пакетов и установит пакет **EASY-RSA:**

**sudo apt update && sudo apt install -y iptables easy-rsa prometheus-node-exporter apache2-utils**

**-** внесет правки в файл конфигурации ssh и установит правила: запрет входа от рута, подключение только по ключам, запрет на подключение по пустому паролю, запрет на подключение по паролю.

* Запустит скрипт **caIPtablesRules.sh**, который применит правила для фаервола.
* Создаст папку где будут располагаться скрипты для работы с созданием сертификатов: **mkdir easy-rsa** .
* Создаст ссылку на нашу созданную папку, чтобы получить все необходимые файлы из шаблонов easy-rsa:

**ln -s /usr/share/easy-rsa/\* ~/easy-rsa/**

и установит права на папку с ограничением для всех кроме владельца командой:

**chmod 700 ~/easy-rsa/ .**

* Командой **./easyrsa init-pki** из директории **~/easy-rsa/** создаст директорию для инфраструктуры публичных ключей в нашей папке и сразу изменит владельца на ней: **chown -R $caUser:$caUser /home/$caUser/easy-rsa/**.
* Затем резвернет файл-шаблон конфигурации **easy-rsa из** deb-пакета **config-file-for-easyrsa.deb**
* Сгенерирует ключ уд. центра запуском скрипта: **./easyrsa build-ca**
* Затем сгенерирует файл запроса сертификата и секретный ключ для vpn-сервера: **./easyrsa gen-req server nopass**
* Подпишет запрос на серверный сертификат для сервера **“server”**:

**./easyrsa sign-req server server**

**-** Далее активирует демон для системы бекапа rsync - в файл **/etc/default/rsync** запишется строка

**RSYNC\_ENABLE=true,** создаст директорию для файлов rsync и сгенерирует файл конфигурации **/etc/rsyncd.conf** где указаны адреса в сети клиентов копирования rsync и директории для бекапа.

**-** Запросит ввести DNS-адреса каждой машины в инфраструктуре. Например ca.ru-central1-a.ru

- Сгенерирует пары ключ - сертификат для экспортеров на машинах CA,VPN,MONITORING,BKP#1,BKP#2 и ключ - сертифика для клиента prometheus.

- Создаст директорию для экспортера прометеус **/opt/node\_exporter/,** перенесет в нее ключ и сертификат для локального экспортера, запросит логин и пароль для подключения к экспортеру (ввести логин admin и пароль), что и будет записано в файл конфигурации **/opt/node\_exporter/web.yml**

- Создаст юнит на автозапуск экспортера и вконце перезапустит сервисы prometheus и alertmanager.

**После этого удостоверяющий центр будет готов к работе.**

* Для подписания запросов клиентов необходимо полученные от пользователей файлы .req помещать в папку **/home/$caUser/easy-rsa/pki/reqs/**
* Затем командой **./easyrsa sign-req client client# (client# - имя пользовательского req-файла без расширения)** мы подписываем запрос клиента.
* Таким образом easyrsa сгенерирует файл client#.crt, который необходимо передать клиенту.