Руководство системного администратора

1. Установить ОС в облаке на 3 сервера (УЦ, VPN, Мониторинг), настроить подключение SSH

2. На сервере УЦ:

sudo apt-get install easy-rsa iptables-persistent

3.Настроить SSH к VPN с УЦ.

(ssh-keygen -t rsa

скопировать содержимое публичного ключа в файл ~/.ssh/authorized\_keys на сервере VPN)

4. Скопировать на УЦ пакеты insteasyrsa.sh, instiptables.sh и запустить. указать порт 9100

5. Переходим на сервер VPN и выполняем:

sudo apt-get install easy-rsa openvpn iptables-persistent

6. Настроить SSH к УЦ с сервера VPN.

(ssh-keygen -t rsa

скопировать содержимое публичного ключа в файл ~/.ssh/authorized\_keys на сервере удостоверяющего центра)

7. Скопировать на VPN пакеты insteasyrsavpn.sh, instiptables.sh и запустить . указать порт 9100, 9167

8. Переходим на сервер УЦ.

Скопировать пакет insteasyrsa2.sh и запустить

9. Перейти на сервер VPN

Скопировать скрипт insteasyrsavpn2.sh и запустить

10. На сервер VPN cкопировать скрипт instopenvpn.sh и запустить

11. Запустить скрипт instnode\_exporter.sh

12. Запустить скрипт instmonitorOpenVPN.sh

13. Перейти на сервер УЦ. Запустить скрипт instnode\_exporter.sh

14. Перейти на сервер мониторинга и выполнить

sudo apt-get install iptables-persistent

15. Скопировать скрипт instiptables.sh и запустить. указать порты 9093, 9090, 9100

16. Запустить скрипт instprometheus.sh

17. Запустить скрипт instnode\_exporter.sh

18. Скопировать пакет instprom\_0.1-1\_all.deb и запустить. В конфигурационных файлах при необходимости изменить адреса серверов, участвующих в мониторинге