Краткая инструкция для системного администратора

Вся инфраструктура располагается в яндекс облаке в организации «organization-i-gilyazev

»

Права доступа:

[I.Gilyazev@yandex.ru](mailto:I.Gilyazev@yandex.ru) - organization-manager.organizations.owner

[Admin@bla.ru](mailto:Admin@bla.ru) – admin

Пароль для пользователя «[Admin@bla.ru](mailto:Admin@bla.ru)» запросить у руководителя it департамента.

Виртуальные сервера располагаются в зоне доступности ru-central1-a и один виртуальный сервер ru-central1-b для надежности

Виртуальные машины:

trust-center – Центр сертификации , ru-central1-a

ovpn-server – Сервер OpenVPN, ru-central1-a

data – локальный репозиторий deb пакетов и хранилище конфиг. Файлов, ru-central1-a

monitor – Prometheus + Grafana, ru-central1-a

epds0n635r2pc0gqfs8n – локальный репозиторий deb пакетов, ru-central1-b

Приватные адреса в подсети 10.128.0.0 /24 в зоне ru-central1-a и 10.129.0.0 /24 в зоне ru-central1-b

Являются динамическими, все сервисы общаются между собой по доменным именам.

Внешние (публичные) адреса также динамические, кроме openvpn сервера. 158.160.100.225 является статическим для openvpn сервера.

Домен у регистратора пока не регистрировался и не делегировался на ns сервера яндекса.

**Подробное описание работы серверов.**

Для подключения к серверам необходимо создать пару ключей с помощью ssh-keygen и отправить публичный ключ на адрес [i.gilyazev@yandex.ru](mailto:i.gilyazev@yandex.ru)

Порт для подключения 22.

***Openvpn сервер:***

Подняты сервисы [openvpn-server@server.service](mailto:openvpn-server@server.service), easy-rsa, Prometheus-node-exporter, openvpn-exporter (работает на порту 9176)

Настроен firewall:

Разрешены вхоящий и проходящий трафик для локального порта на порту 1194 для openvpn, входящий и проходящий трафик для tun интерфейса, настроен nat для tun интерфейса. Разрешен трафик на порту 53, а также разрешен трафик из подсети 10.128.0.0, остальной трафик запрещён.

Поднятие нового сервера:

Создать сервер и подключится к нему, сгенерировать пару ssh ключей без пароля. Открытую часть ключа дописать в файл authorized\_keys на сервере trust-center и подключиться к нему по ssh для принятия фингерпринта.

редактируем файл /etc/sysctl.conf, там нужно снять коментарий с строки net.ipv4.ip\_forward = 1

проверяем sudo sysctl -p должно выдать net.ipv4.ip\_forward = 1

создаем файл для локального репозитория sudo vim /etc/apt/source\_list.d/myrepo.list и дописать туда “ deb [allow-insecure=yes] http://data/myrepo/ mydistr main”

обновляем список пакетов в репозитории и устанавливаем пакет sudo apt-get install config-ovpn -f

Создание конфиг файла для клиента:

/usr/bin/create\_client.sh [имя клиента]

/usr/bin/make\_config.sh [имя клиента]

После этого отправляем его клиенту /opt/openvpn/clients/files/…ovpn

***Trust-center***

Поднят сервис easy-rsa, Prometheus-node-exporter

Создан промежуточный сертификат. /opt/easy-rsa/pki/ca.crt

Настроен firewall:

Разрешен трафик на порту 53,22, а также разрешен трафик из подсети 10.128.0.0, остальной трафик запрещён.

Поднятие нового сервера:

создаем файл для локального репозитория sudo vim /etc/apt/source\_list.d/myrepo.list и дописать туда “ deb [allow-insecure=yes] http://data/myrepo/ mydistr main”

обновляем список пакетов в репозитории и устанавливаем пакет sudo apt-get install easy-rsa-conf -f

Если случится так ,что придётся пересоздать корневой сертификат ,то удаляем корневой сертификат /opt/easy-rsa/pki/ca.crt и запускаем скрипт /usr/bin/install.sh

Соответственно после этого придётся пересоздать все сертификаты для openvpn сервера. (Легче пересоздать сервер)

***Prometeus***

Подняты сервисы Prometheus, prometheus-node-exporter,Grafana.

Prometheus работает на порту 9090, Grafana на порту 3000. Логин для Grafana “admin” пароль у руководителя it.

Настроен мониторинг узлов trust-center:9100,ovpn-server:9100,local-repo:9100,Prometheus:9100,openvpn\_exporter:9176

На Grafana настроены дашборды один для openvpn сервиса. Один типовой для всех узлов.

Также настроены аллерты для всех узлов. Алерты приходят на почтовый адрес [i.gilyazev@yandex.ru](mailto:i.gilyazev@yandex.ru)

Для openvpn сервиса отслеживается статус сервиса (down)

Для серверов отслеживание статуса ноды (down), avg hight (>80%), RAM hight (>80%), rootfs is low (<70%)

Настроен firewall:

Разрешен трафик на порту 53,22, а также разрешен трафик из подсети 10.128.0.0, остальной трафик запрещён.

Поднятие нового сервера:

создаем файл для локального репозитория sudo vim /etc/apt/source\_list.d/myrepo.list и дописать туда “ deb [allow-insecure=yes] http://data/myrepo/ mydistr main”

обновляем список пакетов в репозитории и устанавливаем пакет sudo apt-get install monitoring -f

***Local deb-repo***

Подняты сервисы aptly,nginx

Основной каталог для репозитория на /opt/aptly

Сервисом aptly созданы симлинки пакетов на дерикторию /var/www/aptly/myrepo

Сами пакеты, скрипты и наработки лежат в соответствующих папках в директории /home/ildar

Настроен firewall:

Разрешен трафик на порту 53,22, а также разрешен трафик из подсети 10.128.0.0, 10.129.0.0 остальной трафик запрещён.

Поднятие нового сервера, создаем образ диска с другого сервера и указываем его как загрузчик для новой vm.

Копии пакетов и наработок есть на флешке.

В яндексе настроен Yandex cloud backup и расписание раз в день, раз в неделю и раз в месяц снимаются бекапы с trust-center,ovpn-server,Prometheus.

Так же есть копия сервера local deb-repo и распологается в другой зоне доступности.