

基于docker搭建openvpn

参考资料:

<http://www.acaiblog.cn/2018/12/05/%E5%9F%BA%E4%BA%8Edocker%E6%90%AD%E5%BB%BAoopenvpn/>

环境:

CentOS 7.7

Docker version 19.03.8

防火墙关闭状态

一、容器准备工作

1、安装docker

```
yum install -y yum-utils device-mapper-persistent-data lvm2
yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-
ce.repo
yum install -y docker-ce

[root@localhost ~]# docker -v
Docker version 19.03.6, build 369ce74a3c
```

2、配置阿里云加速器

```
mkdir /etc/docker
vim /etc/docker/daemon.json
```

添加下面内容:

```
{
  "registry-mirrors": ["https://tue4pc99.mirror.aliyuncs.com"]
}
```

```
systemctl start docker #启动
```

```
docker search openvpn #查看镜像
docker pull kylemanna/openvpn #拉取镜像
```

二、启动配置容器

启动容器前，在本地创建openvpn目录用来存放openvpn配置，相当于新建数据卷

```
mkdir /opt/openvpn
```

1、初始化openvpn容器

```
docker run -v /opt/openvpn:/etc/openvpn --rm kylemanna/openvpn ovpn_genconfig -u  
udp://58.210.240.122
```

2、生成证书文件

```
docker run -v /opt/openvpn:/etc/openvpn --rm -it kylemanna/openvpn ovpn_initpki
```

```
init-pki complete; you may now create a CA or requests.  
Your newly created PKI dir is: /etc/openvpn/pki  
  
Generating a 2048 bit RSA private key  
.....+++++  
.....+++++  
writing new private key to '/etc/openvpn/pki/private/ca.key.XXXXELNpeh'  
Enter PEM pass phrase:  
Verifying - Enter PEM pass phrase:  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:acaiblog.cn  
  
CA creation complete and you may now import and sign cert requests.  
Your new CA certificate file for publishing is at:  
/etc/openvpn/pki/ca.crt
```

确认证书认证密码:

```
writing new private key to '/etc/openvpn/pki/private/acaiblog.cn.key.XXXXnMNlip'  
-----  
Using configuration from /usr/share/easy-rsa/openssl-easyrsa.cnf  
Enter pass phrase for /etc/openvpn/pki/private/ca.key:  
Check that the request matches the signature  
Signature ok  
The Subject's Distinguished Name is as follows
```

```
commonName          :ASN.1 12:'acaiblog.cn'
Certificate is to be certified until Dec  2 04:42:08 2028 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
Using configuration from /usr/share/easy-rsa/openssl-easyrsa.cnf
Enter pass phrase for /etc/openvpn/pki/private/ca.key:
An updated CRL has been created.
CRL file: /etc/openvpn/pki/crl.pem
```

三、启动openvpn容器

启动容器

```
docker run -d --name openvpn-server -v /opt/openvpn:/etc/openvpn -p
1194:1194/udp --cap-add=NET_ADMIN --restart always kylemanna/openvpn
```

四、.生成客户端证书

生成客户端无密码证书

```
docker run -v /opt/openvpn:/etc/openvpn --rm -it kylemanna/openvpn easyrsa
build-client-full CLIENTNAME nopass
```

需要输入初始化openvpn-server的认证密码

```
Generating a 2048 bit RSA private key
.....+++++
.....+++++
writing new private key to '/etc/openvpn/pki/private/CLIENTNAME.key.xxxxpIdkeF'
-----
Using configuration from /usr/share/easy-rsa/openssl-easyrsa.cnf
Enter pass phrase for /etc/openvpn/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName          :ASN.1 12:'CLIENTNAME'
Certificate is to be certified until Dec  2 04:48:52 2028 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
```

五、.导出客户端证书

导出客户端证书到/root目录下

```
docker run -v /opt/openvpn:/etc/openvpn --rm kylemanna/openvpn ovpn_getclient
CLIENTNAME > /root/client-acaiblog.cn.ovpn
```

六、开启内核转发

```
[root@localhost ~]# echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf
[root@localhost ~]# sysctl -p
net.ipv4.ip_forward = 1
```

七、openvpn客户端测试

下载地址: <https://swupdate.openvpn.org/community/releases/openvpn-install-2.4.6-l602.exe>

相关命令:

查看运行的容器: `docker ps -a`

停止运行的容器: `docker stop ee8555134f83`

删除停止容器(删除前必须先停止): `docker rm 82ac8a923fa7`