阿里云运维

- 阿里云ECS无公网IP服务器访问外网
- 阿里云+acme.sh+docker容器自动续签证书

阿里云ECS无公网IP服务器访问外网

以下需要在有公网访问权限的服务器上操作

1、开启ECS的路由转发功能

```
echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.conf
sysctl -p
```

2、配置IPTABLES的NAT转发规则

```
# 根据需要进行放通，192.168.20.52/32表示只匹配这一个ip，也可以写整个网段，192.168.20.50表示出去的那台公网服务器的内网ip。
iptables -t nat -I POSTROUTING -s 192.168.20.52/32 -j SNAT --to-source 192.168.20.50
```

3、配置阿里云控制台



4、测试

```
sh-4.1# ping www.baidu.com
PING www.a.shifen.com (180.101.50.242) 56(84) bytes of data.
64 bytes from 180.101.50.242: icmp_seq=1 ttl=49 time=16.8 ms
64 bytes from 180.101.50.242: icmp_seq=2 ttl=49 time=16.7 ms
64 bytes from 180.101.50.242: icmp_seq=3 ttl=49 time=16.7 ms
64 bytes from 180.101.50.242: icmp_seq=4 ttl=49 time=16.8 ms
64 bytes from 180.101.50.242: icmp_seq=5 ttl=49 time=16.7 ms
```

参考资料：

- 【博客园】： 阿里云ECS实现内网服务器访问外网

阿里云+acme.sh+docker容器自动续签证书

由于acme.sh的需要到github下载，但国内有些网络从github下载很慢或者根本就无法下载，就转到docker容器（可以使用阿里云提供的镜像服务加速）

一、创建DNS解析API权限的子账号

登录阿里云控制台：https://ram.console.aliyun.com

添加拥有域名解析权限的子账号，获取AccessKey与AccessSecret

二、使用acme.sh容器生成证书

2.1 初次使用配置

```
# 挂载目录，请设置一个固定的绝对路径，后面都需要使用
ACME_VOLUME="$(pwd)/etc.d"
# 注册账号，请将邮箱替换成你的个人邮箱，在证书申请失败时会发送通知到这个邮箱
sudo docker run --rm  -it -v "${ACME_VOLUME}":/acme.sh --register-account -m acme@example.com
```

2.2 申请证书

```
# 挂载目录
ACME_VOLUME="$(pwd)/etc.d"
# 申请证书
sudo docker run --rm  -it -v "${ACME_VOLUME}":/acme.sh -e Ali_Key=<阿里云AccessKey> -e Ali_Secret=<阿里云密钥>  --net=host
neilpang/acme.sh  --issue --dns dns_ali -d <域名> -d *.<域名>
```

证书申请成功后，在挂载目录`${ACME_VOLUME}/${DOMAIN}`下会有对应的`fullchain.cer`与`<domain>.key`文件。

2.3 添加自动续签任务

添加定时脚本

```
#!/bin/bash

# 请将挂载目录替换成真实目录
ACME_VOLUME="$(pwd)/etc.d"
/usr/bin/sudo /usr/bin/docker run --rm  -it  -v "${ACME_VOLUME}":/acme.sh --net=host  neilpang/acme.sh --cron
# 由于是在docker容器中续签无法控制宿主机的nginx的重新加载，此处直接重新加载好了，反正这个加载速度很快
/usr/bin/sudo /usr/sbin/nginx -t && /usr/bin/sudo /usr/sbin/nginx -s reload
```

添加定时任务

```
# 修改定时任务
crontab -e

# 将脚本替换成真实路径
12 0 * * * /opt/acme.sh/cron.d/nginx.sh
```

参考资料

- 【乱七八糟的开发日常】 - 使用Certbot申请免费泛域名证书
- 【Github】 - 阿里云RAM用户管理多个域名
- 【Github】 - 使用阿里云dns接口申请证书
- 【Github】 - acme.sh