Docker开放远程安全访问（开启2376端口和CA认证）

孙华栋 发布于 2020-03-15

前言

仅仅开放远程访问Docker API，这个还不够的，因为会有安全问题。关于这点，Docker有相关的安全机制，参考官方文档 Protect the Docker daemon socket，大致就是：生成证书，用来达到验证客户端身份的目的。

下面是操作步骤：

服务器配置

1. 创建certs文件夹，用来存放CA私钥和公钥

```
mkdir -pv /etc/docker/certs
cd /etc/docker/certs
```

2. 创建密码

需要连续输入两次相同的密码

```
openssl genrsa -aes256 -out ca-key.pem 4096
```

3. 依次输入密码、国家、省、市、组织名称等（除了密码外其他的可以直接回车跳过）

```
openssl req -new -x509 -days 365 -key ca-key.pem -sha256 -out ca.pem
```

4. 生成server-key.pem

```
openssl genrsa -out server-key.pem 4096
```

5. 生成server.csr（把下面的IP换成你自己服务器外网的IP或者域名）

```
openssl req -subj "/CN=123.123.123.123" -sha256 -new -key server-key.pem -out server.csr
```

6. 配置白名单

0.0.0.0表示所有ip都可以连接。（这里需要注意，虽然0.0.0.0可以匹配任意，但是仍需要配置你的外网ip和127.0.0.1，否则客户端会连接不上）

```
echo subjectAltName = IP:0.0.0.0,IP:123.123.123.123,IP:127.0.0.1 >> extfile.cnf
```

或者也可以设置成域名

```
echo subjectAltName = DNS:www.example.com,IP:123.123.123.123,IP:127.0.0.1 >> extfile.cnf
```

7. 将Docker守护程序密钥的扩展使用属性设置为仅用于服务器身份验证

```
echo extendedKeyUsage = serverAuth >> extfile.cnf
```

8.输入之前设置的密码，生成签名证书

```
openssl x509 -req -days 365 -sha256 -in server.csr -CA ca.pem -CAkey ca-key.pem \
  -CAcreateserial -out server-cert.pem -extfile extfile.cnf
```

9、生成供客户端发起远程访问时使用的key.pem

```
openssl genrsa -out key.pem 4096
```

10. 生成client.csr（把下面的IP换成你自己服务器外网的IP或者域名）

```
openssl req -subj "/CN=123.123.123.123" -new -key key.pem -out client.csr
```

11. 创建扩展配置文件，把密钥设置为客户端身份验证用

```
echo extendedKeyUsage = clientAuth > extfile-client.cnf
```

12. 生成cert.pem，输入前面设置的密码，生成签名证书

```
openssl x509 -req -days 365 -sha256 -in client.csr -CA ca.pem -CAkey ca-key.pem \
  -CAcreateserial -out cert.pem -extfile extfile-client.cnf
```

13. 删除不需要的配置文件和两个证书的签名请求

```
rm -v client.csr server.csr extfile.cnf extfile-client.cnf
```

14. 为了防止私钥文件被更改以及被其他用户查看，修改其权限为所有者只读

```
chmod -v 0400 ca-key.pem key.pem server-key.pem
```

15. 为了防止##### 公钥文件被更改，修改其权限为只读

```
chmod -v 0444 ca.pem server-cert.pem cert.pem
```

16. 修改Docker配置，使Docker守护程序仅接受来自提供CA信任的证书的客户端的连接

拷贝安装包单元文件到/etc，这样就不会因为docker升级而被覆盖

```
cp /lib/systemd/system/docker.service /etc/systemd/system/docker.service
```

在`ExecStart=/usr/bin/dockerd-current \`下面增加

```
--tlsverify \
--tlscacert=/etc/docker/certs/ca.pem \
--tlscert=/etc/docker/certs/server-cert.pem \
--tlskey=/etc/docker/certs/server-key.pem \
-H tcp://0.0.0.0:2376 \
-H unix:///var/run/docker.sock \
```

17. 重新加载daemon并重启docker

```
systemctl daemon-reload
systemctl restart docker
```

客户端配置

1. 创建证书目录

```
mkdir -pv ~/.docker/certs/
cd ~/.docker/certs/
```

2. 将`ca.pem cert.pem key.pem`这3个文件拷贝到当前目录

```
scp ca.pem ./
scp cert.pem ./
scp key.pem ./
```

3. 使用docker客户端测试（注意修改证书路径）

```
docker --tlsverify \
    --tlscacert=/home/alex/.docker/certs/ca.pem \
    --tlscert=/home/alex/.docker/certs/cert.pem \
    --tlskey=/home/alex/.docker/certs/key.pem \
    -H=123.123.123.123:2376 version
```

4. 使用curl测试Docker API

```
curl https://123.123.123.123:2376/images/json \
  --cert ~/.docker/certs/cert.pem \
  --key ~/.docker/certs/key.pem \
  --cacert ~/.docker/certs/ca.pem
```

5. 配置默认远程调用服务器docker服务

```
# 配置~/.zshrc（或者~/.bashrc，根据你的客户端环境而定），在末尾添加以下几行
export DOCKER_HOST=tcp://123.123.123.123:2376 DOCKER_TLS_VERIFY=1
export DOCKER_CERT_PATH=~/.docker/certs/
# 然后让加载到当前会话
source .zshrc
# 测试
docker ps
```

*务必非常小心保管这些key，它们就跟服务器root密码一样重要（众所周知docker是可以进行真实主机提权的）

docker

孙华栋

24 声望　**1** 粉丝

关注作者

0 条评论

得票 最新

撰写评论 ...

提交评论

继续阅读

windows执行docker-compose报错

在Windows 7系统上安装Docker 18.09.3和附带的Docker Compose之后，运行docker-compose命令报错。错误提示如下：

孙华栋　阅读 1.9k

使用IDEA的Docker插件快速实现Docker镜像构建和部署

开发环境 开发环境操作系统：Windows 10 IntelliJ IDEA： 2019.2.4 (Ultimate Edition) Docker服务所在环境：Ubuntu 18.04.4 Server...

孙华栋　赞 3　阅读 11k

开启MySQL远程访问权限 允许远程连接

环境 Ubuntu 18.04 MySQL5.7 登陆mysql数据库 {代码...} 增加远程连接权限 {代码...} 修改MySQL配置文件 {代码...} 注释掉bind-address这行 ...

IMyxuan　赞 4　阅读 8.4k　评论 1

Ubuntu系统Docker环境安装、远程服务开启以及Portainer访问

以下内容有可能需要科学上网才能做到。开始我这里使用的环境是阿里云ecs，系统是Ubuntu 20.04 64位docker 安装...

Lance_Yan 赞 1 阅读 3.8k

【docker】docker 搭建 mongodb3.6，开启授权访问

首先下载mongodb3.6镜像： {代码...} mongodb通常占用27017端口，最简单的启动方式如下： {代码...} 不过通常情况下，我们不会直接这样...

杨成功 赞 1 阅读 4.5k

mysql开启远程访问

说明：Root表示用户名，%代表所有的ip地址，也可以设置指定的ip地址2、在执行 flush privileges;3、查看user表，可以看到： host的值为%...

Abbott 赞 1 阅读 2.3k

Docker开启远程安全访问

一、编辑docker.service文件 {代码...} 找到 [Service] 节点，修改 ExecStart 属性，增加 -H tcp://0.0.0.0:2375 {代码...} 这样相当于对外开放的是...

niceyoo 赞 1 阅读 3.5k

线上mysql服务器开启远程访问

第二步：更改mysql数据库中的user表中的host为%，%意为允许任何ip地址连接只要用户的账号密码正确。[PHP] 纯文本查看 复制代码?1use...

林晓邬 阅读 505