# 防火墙

**# 开启防火墙**service firewalld start**#重启防火墙**service firewalld restart**#关闭防火墙**service firewalld stop

### 开启防火墙指定端口

firewall-cmd --zone=public --add-port=80/tcp --permanent  
---  
firewall-cmd --zone=public --add-port=5672/tcp --permanent   # 开放5672端口  
  
firewall-cmd --zone=public --remove-port=5672/tcp --permanent  #关闭5672端口  
  
firewall-cmd --reload # 配置立即生效

**# 参数解释**1、firwall-cmd：是Linux提供的操作firewall的一个工具；2、–permanent：表示设置为持久；3、–add-port：标识添加的端口；

**#查询指定端口是否开放**firewall-cmd --query-port=80/tcp （可将80换为自己想要查询的指定端口号）**#移除端口**firewall-cmd --permanent --remove-port=80/tcp

### 重载防火墙

firewall-cmd --reload

### 验证开放的端口

firewall-cmd --query-port=80/tcp

<https://blog.csdn.net/qq_39100456/article/details/127452292>

-------

## 端口不通

### 关闭SELinux

#### 临时关闭：setenforce 0

#### 修改配置文件：（需要重启机器）

修改/etc/selinux/config 文件

将SELINUX=enforcing改为SELINUX=disabled

第三种：目标端口被IPv6监听，修改到IPv4监听

查看端口的监听情况：netstat -anp |grep 3306

[CENTOS7 可以PING通，但是端口不通情况总结](https://blog.csdn.net/chenwei3390/article/details/114304481)

----------

## docker

Firewalld服务启动时,会将iptables上的规则全部清空，并把firewalld上的防火墙策略规则写入到iptables中，此时docker因为防火墙规则被删除就会不正常，需要重启systemctl restart docker服务来重新刷写防火墙规则到iptables上,在管理Docker端口时，应该使用iptables防火墙而不是firewalld防火墙服务

————————————————

原文链接：<https://blog.csdn.net/weixin_43876317/article/details/122534937>

所以我们安装docker的时候需要先设置这个参数为1,在装docker命令如下：

sysctl -w net.ipv4.ip\_forward=1

sed -i "/net.ipv4.ip\_forward/ s/0/1/g" /etc/sysctl.conf

sysctl -p 命令让内核参数修改生效

net.bridge.bridge-nf-call-ip6tables=1  
net.bridge.bridge-nf-call-iptables=1  
net.bridge.bridge-nf-call-arptables=1  
net.ipv4.ip\_forward=1

<https://zhuanlan.zhihu.com/p/562155940>

<https://www.jb51.net/article/200014.htm>

还要关注下docker 默认网络网段

docker network inspect bridge