

命令总结:

systemctl status firewalld 查看防火墙状态
systemctl start firewalld 开启防火墙
systemctl stop firewalld 关闭防火墙
firewall-cmd --permanent --zone=public --add-port=27017/tcp --permanent 开启指定端口
firewall-cmd --zone=public --remove-port=27017/tcp --permanent 关闭指定端口
firewall-cmd --permanent --zone=public --add-port=27017-30000/tcp --permanent 开启指定范围端口
firewall-cmd --permanent --zone=public --add-port=1-65535/tcp --permanent 开始所有端口
firewall-cmd --zone=public --remove-port=27017-30000/tcp --permanent 关闭指定范围端口
firewall-cmd --permanent --query-port=27017/tcp 查看端口是否开放
firewall-cmd --reload 重启防火墙
firewall-cmd --list-ports 查看已经开放的端口
iptables -L -n 查看规则, 这个命令是和iptables的相同的
man firewall-cmd 查看帮助

常用命令说明

1、通过systemctl status firewalld查看firewalld状态, 发现当前是dead状态, 即防火墙未开启。

```
[root@instance-kbs6ip7o bin]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
   Active: inactive (dead)
   Docs: man:firewalld(1)

Dec 11 14:18:31 instance-kbs6ip7o systemd[1]: Starting firewalld - dynamic firewall daemon...
Dec 11 14:18:32 instance-kbs6ip7o systemd[1]: Started firewalld - dynamic firewall daemon.
Dec 11 15:09:29 instance-kbs6ip7o systemd[1]: Stopping firewalld - dynamic firewall daemon...
Dec 11 15:09:29 instance-kbs6ip7o systemd[1]: Stopped firewalld - dynamic firewall daemon.
```

2、通过systemctl start firewalld开启防火墙, 没有任何提示即开启成功

```
[root@instance-kbs6ip7o bin]# systemctl start firewalld
[root@instance-kbs6ip7o bin]#
```

3、再次通过systemctl status firewalld查看firewalld状态, 显示active (running) 即已开启了

```
[root@instance-kbs6ip7o bin]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
   Active: active (running) since Tue 2018-12-11 15:13:46 CST; 1min 16s ago
   Docs: man:firewalld(1)
  Main PID: 28282 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─28282 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

Dec 11 15:13:46 instance-kbs6ip7o systemd[1]: Starting firewalld - dynamic firewall daemon...
Dec 11 15:13:46 instance-kbs6ip7o systemd[1]: Started firewalld - dynamic firewall daemon.
[root@instance-kbs6ip7o bin]#
```

4、如果要关闭防火墙设置, 可能通过systemctl stop firewalld这条指令来关闭该功能, 没有任何提示则关闭成功

```
[root@instance-kbs6ip7o bin]# systemctl stop firewalld
[root@instance-kbs6ip7o bin]#
```

5、开启端口，再次执行执行firewall-cmd --permanent --zone=public --add-port=27017/tcp --permanent，提示success，表示设置成功，这样就可以继续后面的设置了。

```
[root@instance-kbs6ip7o bin]# firewall-cmd --zone=public --add-port=27017/tcp --permanent  
success
```

注：可以是一个端口范围，如1000-2000/tcp

移除端口：firewall-cmd --zone=public --remove-port=80/tcp --permanent

6、查看端口，执行firewall-cmd --permanent --query-port=27017/tcp，提示yes，即查询成功

```
[root@instance-kbs6ip7o bin]# firewall-cmd --permanent --query-port=27017/tcp  
yes  
[root@instance-kbs6ip7o bin]#
```

7、重启防火墙，执行firewall-cmd --reload，提示success即执行成功

```
[root@instance-kbs6ip7o bin]# firewall-cmd --reload  
success  
[root@instance-kbs6ip7o bin]#
```

--zone #作用域

--add-port=80/tcp #添加端口，格式为：端口/通讯协议

--remove-port=80/tcp #移除端口，格式为：端口/通讯协议

--permanent #永久生效，没有此参数重启后失效