



链滴

CentOS7 防火墙 firewalld

作者: [ZFIREH](#)

原文链接: <https://ld246.com/article/1559063407064>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)



CentOS升级到7之后，发现无法使用iptables控制Linuxs的端口，google之后发现Centos 7使用firealld代替了原来的iptables。下面记录如何使用firewalld：

1. firewalld的基本使用

```
#启动：
systemctl start firewalld
#关闭：
systemctl stop firewalld
#查看状态：
systemctl status firewalld
#开机禁用：
systemctl disable firewalld
#开机启用：
systemctl enable firewalld
```

2. systemctl是CentOS7的服务管理工具中主要的工具 它融合之前service和chkconfig的功能于一体

```
#启动一个服务：
systemctl start firewalld.service
#关闭一个服务：
systemctl stop firewalld.service
#重启一个服务：
systemctl restart firewalld.service
#显示一个服务的状态：
systemctl status firewalld.service
#在开机时启用一个服务：
systemctl enable firewalld.service
#在开机时禁用一个服务：
```

```
systemctl disable firewalld.service
#查看服务是否开机启动:
systemctl is-enabled firewalld.service
#查看已启动的服务列表:
systemctl list-unit-files|grep enabled
#查看启动失败的服务列表:
systemctl --failed
```

3. 配置firewalld-cmd

```
# 查看版本:
firewall-cmd --version
# 查看帮助:
firewall-cmd --help
# 显示状态:
firewall-cmd --state
# 查看所有打开的端口:
firewall-cmd --zone=public --list-ports
# 更新防火墙规则:
firewall-cmd --reload
# 查看区域信息:
firewall-cmd --get-active-zones
# 查看指定接口所属区域:
firewall-cmd --get-zone-of-interface=eth0
# 拒绝所有包:
firewall-cmd --panic-on
# 取消拒绝状态:
firewall-cmd --panic-off
# 查看是否拒绝:
firewall-cmd --query-panic
# 重新载入
firewall-cmd --reload
```

4. 开启一个端口

```
[root@zhouhuoc ~] firewall-cmd --zone=public --add-port=80/tcp --permanent
[]
```

命令含义: --zone #作用域

--add-port=80/tcp #添加端口, 格式为: 端口/通讯协议

--permanent #永久生效, 没有此参数重启后失效

5. 重新载入防火墙

```
[root@zhouhuoc ~] firewall-cmd --reload
```

6. 查看端口是否开放

```
[root@zhouhuoc ~] firewall-cmd --zone= public --query-port=80/tcp
```

7. 将端口从开放列表移除

```
[root@zhouhuoc ~] firewall-cmd --zone= public --remove-port=80/tcp --permanent
```

参考文档:

1. [CentOS7使用firewalld打开关闭防火墙与端口](#)