

# 防火墙配置脚本

脚本位于 `/shell/firewall.sh`

## 1. 功能简介

此脚本有两个主要功能：

1. **配置防火墙白名单**：将集群节点 IP、集群 IP CIDR、POD IP CIDR 以及一个额外 IP 地址加入到防防火墙的白名单中
2. **删除配置**

## 2. 使用方法

### 2.1 显示帮助信息

在终端中执行以下命令：

```
bash ./firewall.sh -h
```

将显示帮助信息。

### 2.2 配置白名单

在终端中执行以下命令：

```
bash ./firewall.sh -e <pod cidr> <other cidr>
```

将生成白名单配置。关于为什么只用输入 pod cidr 不需要输入其他 k8s 相关 ip，见 3.1 节。

### 2.3 删除配置

在终端中执行以下命令：

```
bash ./firewall.sh -d
```

将删除白名单配置。

## 3. 实现说明

### 3.1 配置白名单

此脚本使用了 firewalld 防火墙的 zone 机制，`-e` 选项将直接生成 firewalld trusted zone 的配置文件（默认情况下，trusted zone 配置文件不存在），并将对应的 ip 地址加入到该 zone 中。

关于参数输入 ip 的说明：

node ip、集群 ip 都可以查询 k8s 配置文件或使用 `kubectl` 命令获取，但是没有找到 pod ip 的获取方法，鉴于 pod ip cidr 在集群创建时指定，认为用户应当知晓 pod ip cidr，所以作为参数输入。

### 3.2 删除配置

`-d` 选项将直接删除 trusted zone 配置文件。