# Linux systemctl 管理服务、防火墙 firewalld 以及 SELinux 配置

主讲教师：（大地）
合作网站：www.itying.com （IT 营）
我的专栏：https://www.itying.com/category-79-b0.html

一、 使用 systemctl 管理服务.....1

二、 Firewalld 防火墙的设置.....2

三、 SELinux 防火墙的设置.....3

## 一、使用 systemctl 管理服务

**systemctl** 就是 service 和 chkconfig 这两个命令的整合，在 **CentOS 7** 就开始被使用了，**systemctl** 是系统服务管理器命令，它实际上将 service 和 chkconfig 这两个命令组合到一起。

| 任务 | 旧指令 | 新指令 |
| --- | --- | --- |
| 使某服务自动启动 | chkconfig --level 3 httpd on | systemctl enable httpd.service |
| 使某服务不自动启动 | chkconfig --level 3 httpd off | systemctl disable httpd.service |
| 检查服务状态 | service httpd status | systemctl status httpd.service（服务详细信息） systemctl is-active httpd.service（仅显示是否 Active） |
| 显示所有已启动的服务 | chkconfig --list | systemctl list-units --type=service |
| 启动某服务 | service httpd start | systemctl start httpd.service |
| 停止某服务 | service httpd stop | systemctl stop httpd.service |
| 重启某服务 | service httpd restart | systemctl restart httpd.service |

**Syetemclt 管理服务常用命令**

1、启动服务：systemctl start httpd

2、关闭服务：systemctl stop httpd

3、重启服务：systemctl restart httpd

3、查看一个服务的状态：systemctl status httpd

4、查看一个服务是否在运行：systemctl is-active httpd

5、查看当前已经运行的服务：systemctl list-units -t service

6、列出所有服务： systemctl list-units -at service 注意顺序

8. 设置开机自启动： systemctl enable httpd

9. 停止开机自启动： systemctl disable httpd

10、列出所有自启动服务：

systemctl list-unit-files|grep enabled
systemctl list-unit-files|grep disabled
systemctl list-unit-files|grep disabled | grep httpd

11、使指定服务从新加载配置：systemctl reload httpd

# 二、Firewalld 防火墙的设置

从 CentOS7(RHEL7)开始，官方的标准防火墙设置软件从 iptables 变更为 firewalld，相信不少习惯使用 iptables 的人会感到十分不习惯，但实际上 firewalld 更为简单易用。

**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

**配置 firewall-cmd :**

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

**那怎么开启一个端口呢:**

firewall-cmd --zone=public --add-port=80/tcp --permanent （－permanent 永久生效，没有此参数重启后失效）

**重新载入:**

firewall-cmd --reload 修改 firewall-cmd 配置后必须重启

**查看:**

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

**删除:**

firewall-cmd --zone= public --remove-port=80/tcp --permanent

# 三、SELinux 防火墙的设置

安全增强型 Linux（Security-Enhanced Linux）简称 SELinux，它是一个 Linux 内核模块，也是 Linux 的一个安全子系统。

SELinux 主要由美国国家安全局开发。2.6 及以上版本的 Linux 内核都已经集成了 SELinux 模块。

SELinux 的结构及配置非常复杂，而且有大量概念性的东西，要学精难度较大。很多 Linux 系统管理员嫌麻烦都把 SELinux 关闭了。阿里云安装的 centos 默认已经关闭了。西部数码云服务器默认也是关闭的。

## 查看 SELinux 状态:

```
1、/usr/sbin/sestatus -v      ##如果 SELinux status 参数为 enabled 即为开启状态
SELinux status:                 enabled
2、getenforce                   ##也可以用这个命令检查
```

## 关闭 SELinux：

1、临时关闭（不用重启机器）：

```
setenforce 0                    ##设置 SELinux 成为 permissive 模式
setenforce 1 设置 SELinux 成为 enforcing 模式
```

**2、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
```