**系统安全保护**

selinux安全机制

selinux概述

selinux美国NSA国家安全局主导研发，一套增强linux系统安全的强制访问控制体系

集成到Linux内核中运行

RHEL7基于selinux体系针对用户、进程、目录和文件提供了预设的保护策略，以及管理工具

selinux运行模式的切换

enforcing（强制，有效，会做出禁止、警告等动作）

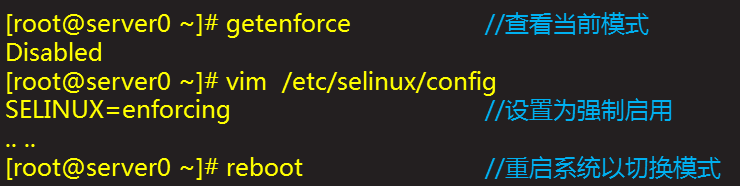
permissive（宽松，不限制做任何操作，但会记录下来）

disabled（彻底禁用，变成disable的模式都需要更改配置文件并重启）

切换运行模式

临时切换：setenforce 1|0

固定配置：/etc/selinux/config文件

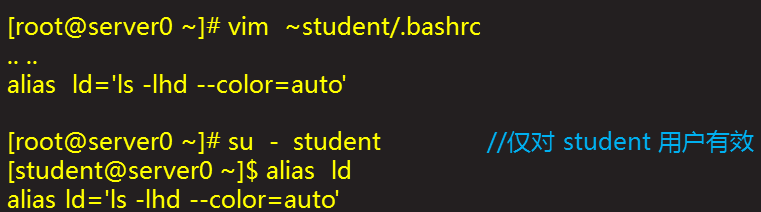


**配置用户环境**

用户初始化文件

用户个性化配置文件

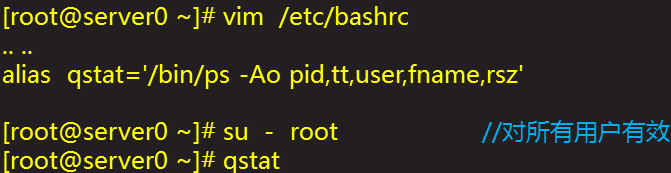
~/.bashrc，每次开启bash终端时生效



全局环境配置

影响所有用户的bash解释环境

/etc/bashrc，每次开启bash终端时生效

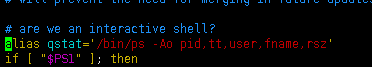


自定义命令









**防火墙策略管理（过滤性）**

**作用：隔离，过滤入站请求，允许出站**

**分类：硬件防火墙**

**软件防火墙**

firewalld服务基础

搭建两个服务：web、ftp

web：1.服务端虚拟机sever，安装可以提供web服务的软件

apache（httpd） nginx tomcat

yum -y install httpd

1. 虚拟机server操作，启动httpd服务，设置为开机自启



1. 本机测试访问



1. 书写页面

默认路径：/var/www/html/



ftp：1.服务端虚拟机sever，安装可以提供web服务的软件

yum -y install vsftpd

1. 启动服务



1. 测试

默认共享的路径/var/ftp



RHEL7的防火墙体系

系统服务：firewalld

管理工具：firewall-cmd、firewall-config



**匹配规则的原则：匹配及停止**

预设安全规则

根据所在的网络场所区分，预设保护规则集

public：仅允许访问本机的sshd、dhcp、ping等少数几个服务

trusted：允许任何访问

block：阻塞任何来访请求，明确拒绝

drop：丢弃任何来访的数据包，节省资源

防火墙决定客户端请求进入某个区域的规则：

1. 查看客户端请求中源IP地址，再看所有区域中，哪一个区域有该源IP的规则，则进入该区域（先看源IP，再看有没有源IP对应的策略，如果有，则直接进入该区域，如果没有，进入默认区域）
2. 进入默认区域，public

配置规则的位置

运行时（runtime）

永久（permanent）

查看防火墙规则列表

列表查看操作

firewall-cmd --list-all [--zone=区域名]

firewall-cmd --list-all-zones

firewall-cmd --get-zones

firewall-cmd --get-services

firewall-cmd --get-default-zone

配置防火墙

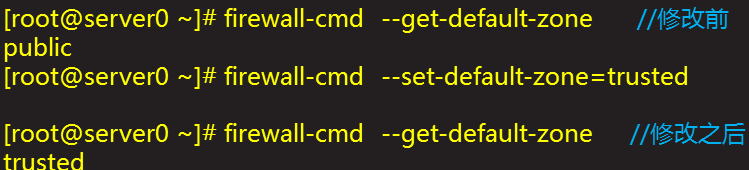
指定默认安全区域

使用set-default-zone=区域名

默认为public，限制较为严格

对于开放式环境，建议将默认区域修改为trusted

针对“运行时/永久配置均有效”

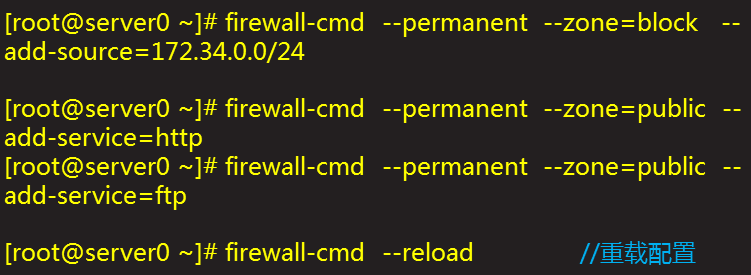


封网段、开服务

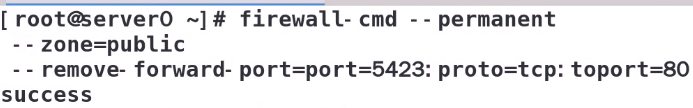
若针对“永久配置”，需添加--permanent

使用--add-source=网段地址

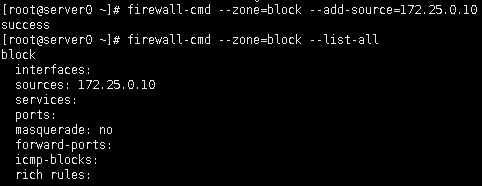
使用--add-service=服务名



remove删除



添加源IP的规则设置（禁止某一IP访问）



工作时防火墙，设置的方式

严格：默认区域为drop，把允许的IP单独放入trusted里面

宽松：默认区域为trusted，把拒绝的IP单独放入drop里面

防火墙功能：实现本机的端口映射（端口转换）

本地应用的端口重定向（端口1-->端口2）

从客户机访问端口1的请求，自动映射到本机端口2

