### 系统安全保护

* SElinux的运行模式

Enforcing（强制） permissive（宽松）disabled（彻底禁用）

任何状态变成disabled， 都必须通过重起reboot

Getenforce 查看状态

切换运行模式

临时切换：setenforce 1|0

固定配置： /etc/selinux/config

[root@server0 ~]# vim /etc/selinux/config #下一次开机后生效

SELINUX=permissive

[root@server0 ~]# setenforce 0 临时生效

修改selinux的运行模式为permissive

[root@server0 ~]# getenforce

Permissive

* 用户初始化文件

• 影响指定用户的 bash 解释环境

– ~/.bashrc,每次开启 bash 终端时生效

• 影响所有用户的 bash 解释环境– /etc/bashrc,每次开启 bash 终端时生效

[root@server0 ~]# vim /root/.bashrc

Alias haha=’echo haha’

[root@server0 ~]# vim /home/student/.bashrc

Alias hehe=’echo hehe’

[root@server0 ~]# vim /etc/bashrc

Alias xixi=’echo xixi’

Root可以执行：haha xixi

Student可以执行：hehe xixi

### 配置高级连接

* 配置聚合连接：（网卡绑定、链路聚合）

作用：网卡设备的冗余

热备份（activebackup）连接冗余

1、创建虚拟的网卡team0 （参考 man teamd.conf 全文搜索/example）

nmcli connection add type team con-name team0 ifname team0 autoconnect yes config '{"runner": {"name": "activebackup"}}'

注释： nmcli connection 添加 类型为team 配置文件名字 team0 ifconfig 显示的名字为team0 每次开机自动启用配置 热备份方式

1. 添加成员：

[root@server0 ~]# nmcli connection add type team-slave con-name team0-1 ifname eth1 master team0

[root@server0 ~]# nmcli connection add type team-slave con-name team0-2 ifname eth2 master team0

注释：nmcli connection 添加 类型为 team的奴隶设备 配置文件名为 team0-1 奴隶的网卡名为eth1 加入的组织为team0

1. 配置ip地址

nmcli connection modify team0 ipv4.method manual ipv4.addresses 192.168.1.1/24 connection.autoconnect yes

1. 激活配置

[root@server0 ~]# nmcli connection up team0

[root@server0 ~]# nmcli connection up team0-1

[root@server0 ~]# nmcli connection up team0-2

1. 验证

[root@server0 ~]# teamdctl team0 state

[root@server0 ~]# ifconfig eth1 down

[root@server0 ~]# teamdctl team0 state

1. 删除配置

[root@desktop0 ~]# nmcli connection delete team0

### 配置ipv6地址

Nslookup 查看解析的ip地址

Ip地址：唯一标识网络中主机

Ipv4地址：

32个二进制 点分十进制，分成4段，最后用点分隔 用10进制表示

Ipv6地址：

128个二进制：分成8段 最后用冒号分隔 用16进制表示

1、配置ipv6地址：

[root@desktop0 ~]# nmcli connection modify 'System eth0' ipv6.method manual ipv6.addresses 2003:ac18::305/64 connection.autoconnect yes

2、激活：[root@desktop0 ~]# nmcli connection up 'System eth0'

3、测试ip 是否能够通信：[root@desktop0 ~]# ping6 2003：ac18::305

### 防火墙策略管理

搭建基本web服务

服务端：虚拟机Server0

1. 安装一个可以提供Web功能软件

[root@server0 ~]# yum -y install httpd

2、启动服务

[root@server0 ~]# systemctl restart httpd 重启httpd服务

[root@server0 ~]# systemctl enable httpd 随机自启服务

1. 书写自己的页面文件

默认存放网页的路径：/var/www/html

默认网页文件的名字：index.html

[root@server0 ~]# vim /var/www/html/index.html

<font color=blue><h1><marquee> 人个有命，上天注定 这个世界并没有我们想象的那么简单

[root@server0 ~]# firefox 172.25.0.11

搭建基本FTP服务（文件传输）：

1、安装一个可以提供Web功能软件

[root@server0 ~]# yum -y install vsftpd

2、启动服务

[root@server0 ~]# systemctl restart vsftpd 重启vsftpd服务

[root@server0 ~]# systemctl enable vsftpd 随机自启服务

1. 默认vsftpd共享的路径：/var/ftp

[root@server0 ~]# firefox ftp：//172.25.0.11

客户端：虚拟机server0

### 防火墙策略的应用

隔离作用

允许出站，过滤入站

硬件防火墙

软件防火墙

系统服务：firewalld

管理工具：firewall-cmd 、firewall-config（图形）

预设安全区域

根据所在网络的网络场所区分，预设保护规则集

public：仅允许访问本机的sshd等少数几个服务

trusted：允许任何访问

block：阻塞任何来访请求（明确回应拒绝）

drop：丢弃任何来访的数据包（没有明确回应，直接丢弃）

防火墙的判断规则：匹配及停止

1. 看客户端请求中的来源的ip地址，查看本身所有区域的规则，如果有一个区域规则有该ip地址的规则，则进入该区域
2. 进入默认区域（一般为public）

查看当前默认区域：

[root@server0 ~]# firewall-cmd --get-default-zone

修改默认区域：

[root@server0 ~]# firewall-cmd --get-default-zone

[root@desktop0 ~]# ping -c 2 172.25.0.11 能通信

[root@server0 ~]# firewall-cmd --set-default-zone=drop

[root@desktop0 ~]# ping -c 2 172.25.0.11 不能通信，且没有回应

[root@server0 ~]# firewall-cmd --set-default-zone=block

[root@desktop0 ~]# ping -c 2 172.25.0.11 不能通信，有回应

常见的协议： 默认端口

http：超文本协议 80

https：安全的超文本传输协议 443

ftp ： 文本传输协议 21

tftp: 简单的文件传输协议 69

telnet ：远程管理协议（路由器，交换机） 23

dns ：域名解析协议 53

smtp：邮件协议 25

pop3：邮件接收协议 110

snmp：简单的管理协议 161

服务案例：

虚拟机server0

[root@server0 ~]# firewall-cmd --zone=public --list-all 查看区域策略

虚拟机Desktop0

[root@localhost ~]# firefox 172.25.0.11

[root@localhost ~]# firefox ftp://172.25.0.11

虚拟机server0

[root@server0 ~]# firewall-cmd --zone=public --list-all 查看区域策略

[root@server0~]#firewall-cmd --zone=public --add-service=http

添加http协议

[root@server0~]#firewall-cmd --zone=public --add-service=ftp

添加ftp协议

虚拟机Desktop0

[root@localhost ~]# firefox 172.25.0.11

[root@localhost ~]# firefox ftp://172.25.0.11

防火墙策略永久配置：

--peamanent 永久设置

[root@server0 ~]# firewall-cmd --reload 重新加载防火墙策略

[root@server0 ~]# firewall-cmd --zone=public --list-all [root@server0 ~]# firewall-cmd --permanent --zone=public --add- service = ftp 添加ftp协议 让其永久生效

success

[root@server0 ~]# firewall-cmd --reload 刷新策略

success

[root@server0 ~]# firewall-cmd --zone=public --list-all

防火墙对于客户端源ip的控制：

拒绝172.25.0.10访问本机的所有服务，其他客户端都可以

虚拟机desktop0

[root@desktop0 ~]# firefox 172.25.0.11 #可以

虚拟机Server0

# firewall-cmd --zone=block --list-all

# firewall-cmd --permanent --zone=block --add-source=172.25.0.10

# firewall-cmd --reload success

# firewall-cmd --zone=block --list-all

虚拟机desktop0

[root@desktop0 ~]# firefox 172.25.0.11 #不可以

### 防火墙处理端口转发功能

服务或者协议的端口：标识服务或者协议

源ip地址 目的ip地址 目标端口号

[root@server0 ~]# firewall-cmd --permanent --zone=public --add-forward-port=port=5423:proto=tcp:toport=80

[root@server0 ~]# firewall-cmd --reload

[root@server0 ~]# firewall-cmd --zone=public --list-all

虚拟机Desktop0 访问 虚拟机Server0 5423端口

将访问 虚拟机Server0 5423端口的请求 转发到 虚拟机Server0 80端口

虚拟Desktop0 ------->172.25.0.11:5423

虚拟机Server0 -----172.25.0.11:5423------>172.25.0.11:80

虚拟机Server0

# firewall-cmd --permanent --zone=public

--add-forward-port=port=5423:proto=tcp:toport=80

# firewall-cmd --reload

# firewall-cmd --zone=public --list-all

虚拟机Desktop0

# firefox 172.25.0.11:5423