Mbr/msddos分区模式

1～4主分区或者1～3个主分区+1扩展分区（n个逻辑分区）

最大支持容量为2.2T的磁盘，扩展分区不能格式化

fdisk分区工具

查看分区表 fdisk -l /dev/sda

修改硬盘的分区表 fdisk /dev/sda

识别新分区表 partprobe

当硬盘的分区表被修改之后，需要将分区表的变化及时通知linux内核，最好reboot一次

格式化分区

Mkfs：ext3、ext4、xfs、vfat -F 32 分区设备路径

刷新文件系统的方式

ext4文件系统: resize2fs

Xfs文件系统: xfs\_growfs

访问已格式化的分区

使用mount命令挂载 mount /dev/vdb2 /mnt/part2

使用df检查使用情况

LVM的工作方式

零散空闲存储-----整合的虚拟磁盘——----------虚拟的分区

PV VG LV

LVM卷组修改PE大小 vgcreate -s 16M datastore /dev/vdb6

环境变量 产建的环境变量PWD、PATH、USER、LOGNAME、SHELL、HOME

Which nmcli //查看命令程序存在哪

检查文件状态

-e 文档是否存在、 -d 目录是否存在、-f 文件是否存在、-r、-w、-x 可读、可写、可执行

检查输入的值是否为空 -z if [ -z $1 ]

$?上一句话的状态值 [ $USER == ‘student’ ]

$！上一个命令运行的PID cp -a $1 $2 killall $!

$\* 所有位置变量的输出

$#所有位置变量输出的个数

$$是脚本当前运行进程的PID号

利用命令的替换取值

For a in seq$\* for的后面不能写{1..$#}引用变量用seq

使用$（命令行）操作

For a in $(cat /root/userlist)

用户初始化文件

普通用户：~student/.bahrc root用户：~root/.bashrc

全剧环境配置: /etc/bashrc

另外,/etc/profile中设定的变量(全局)的可以作用于任何用户,而~/.bashrc等中设定的变量(局部)只能继承/etc/profile中的变量,他们是"父子"关系.

Linux7的防火墙

系统服务:firewalld、firewall-cmd、freiwall-config

根据所在的网络场所区分、与蛇保护规则集

-public：机允许访问本机的sshd等少数几个服务

-trusted：允许任何访问

-block：阻塞任何来访

Linux6的防火墙

系统服务:iptables

raw（状态跟踪表） mangle(打标记) nat(地址转换) filter(过滤表)

PREROUTING PREROUTING PREROUTING INPUT

OUTPUT POSTROUTING POSTROUTING FORWARD

INPUT OUTPUT OUTPUT

PUTPUT

FORWARD

Iptables的四张表：

raw表：对发送来ip包状态的跟踪

//(Prerouting,Output链)

mangle表：给到达防火墙的ip包打标签（标记）

//五种链

Nat表：源地址、目标地址、端口转换

//（input，Prerouting，Postrouting，Output链）

Filter表：过滤ip包

//（Input，Forward，Output链）

Iptables的五种链（ip包传输的方向）

Input链：匹配进入防火墙的包

Output：匹配从防火墙出去的包

Forward：匹配经过防火墙的包

Postrouting：匹配路由后（确定路线,不知道怎么走）

Prerouting：匹配路由前（指路，不确定路线）

基本的目标操作

ACCEPT：允许通过/放行

DROP：直接丢弃，不给任何回应

REJECT：拒绝通过，必要时会给出提示

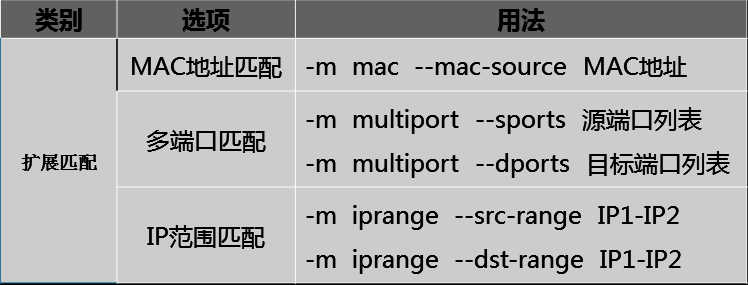
LOG：记录日至，然后传给下一条规则

Iptable的基本用法

Iptables -t 表名 选项 [链名] [条件] [-j目标操作]







Iptables -D INPUT 3 //删除第三行规则

Iptables (-t filter) -A INPUT -p tcp(icmp、udp) -j ACCEPT

Iptables -A INPUT -p icmp ! --icmp-type echo-request -j DROP

多端口案例：

Iptables -A INPUT -p tcp -m multiport --dports 20:22,25,80,110,143,16501:16800 -j ACCEPT //20:22修改端口

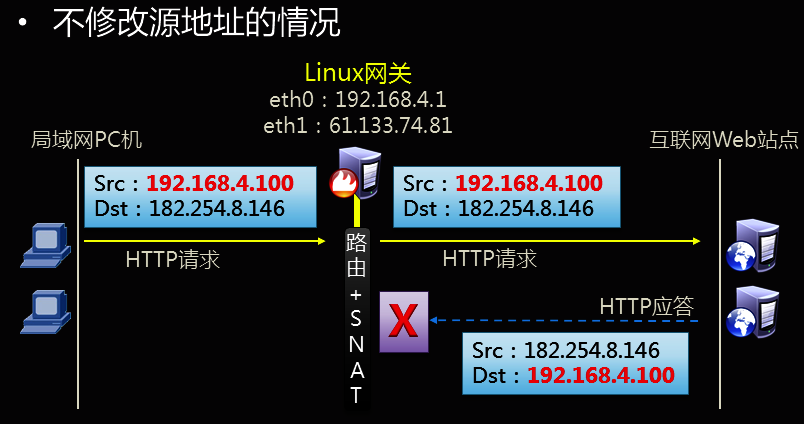
ssh登陆的IP范围控制

允许从192.168.4.10-192.168.4.20登陆

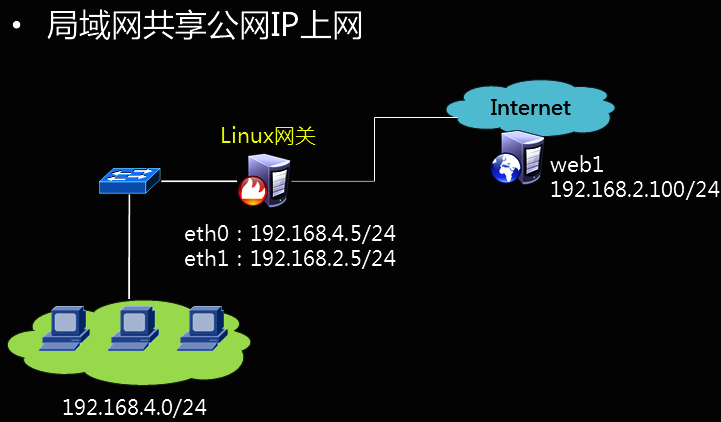
Iptables -A INPUT -p 22 -m iprange --src-range 192.168.4.10-192.168.4.20 -j ACCEPT

SNAT源地址转换

修改数据包的源地址，仅用于nat表的POSTROUTING链



环境



配置的关键策略

选择路由之后，针对来自局域网，即将从外王接口发出取的包，将源IP地址修改位网关的公网IP地址

Iptables -t nat -A POSTROUTING -s 192.168.4.0/24 -p tcp --dport 80 -j SNAT --to-source 192.168.2.5

存储技术分类

SCSI小型计算机系统接口

DAS直连式存储 存储设备通过SCSI或光纤通道值直接连接到计算机上

NAS网络技术存储

SAN存储区域网络

FC光纤通道

NAS技术是一种专用数据存储服务器，以数据为中心。将存储设备与服务器彻底分离，集中管理数据，从而释放带宽提高性能，降低总拥有成本。采用标准的NFS/HTTP/CIFS（smb）等 （服务器与存储设备要有网线相连）

用户通过tcp/ip协议访问数据

samba:装包、创建用户pdbedit -a(-x、-b)添加用户、修改配置文件、selinux值setsebool值的修改(-a 查询)

semanage post -a -t http\_port\_t -p tcp 8909 添加非默认端口(-l 查询)

客户：cifs 挂载，如果是普通用户要提供多用户认证支持。

NFS :装包，配置exports 路径 \*（权限，no\_root\_squash）,重启服务

showmount -e

　　no\_root\_squash：当登录NFS主机使用共享目录的使用者是root时，其权限将被转换成为匿名使用者，通常它的UID与GID都会变成nobody身份。  
　　root\_squash；如果登录NFS主机使用共享目录的使用者是root，那么对于这个共享的目录来说，它具有root的权限。

SAN技术通过光纤交换机、光纤路由器、光纤集线器等设备将磁盘阵列、磁带等存储设备与相关服务器连接起来，形成高速专用网络。 （没有距离的限制）

接口：SCSI、FC 通信协议：IP、SCSI

FC交换机交换拓扑

点到点：point-to-point

简单敬爱嗯两个设备互连

已裁定的环路：arbitrated loop

可多达126个设备共享一段通信或环路

交换式拓扑：switched fabric

所有设备通过光纤交换机互连

ISCSI技术（internet scsi）

TETF指定的标准，将SCSI数据块映射位以太网数据包

将存储网络广泛应用的SCSI接口技术与IP网络相结合

可以在IP网络上构建SAN

解决了传输效率、存储容量、兼容性、安全性等方面的问题

FC SAN 光纤路由器、光纤交换机

IP SAN 投资更低

ISCSI Initiator：软件实现，成本低，性能较低

ISCSI HBA：硬件实现，性能好，成本较高

多路径的配置概述

安装软件包 device-mapper-multipath

使用mpaththconf命令创建配置文件并使用多路径

Mpathconf --user\_friendly\_names n

获取WWID，假如共享存储在本地识别位/dev/sdb和/dev/sdc，

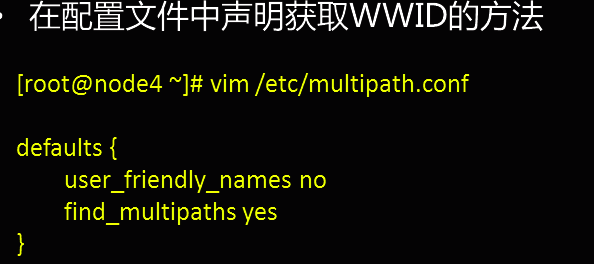
/lib/udev/scsi\_id --withelisted --device=/dev/sdb

/lib/udev/scsi\_id --withelisted --device=/dev/sdc

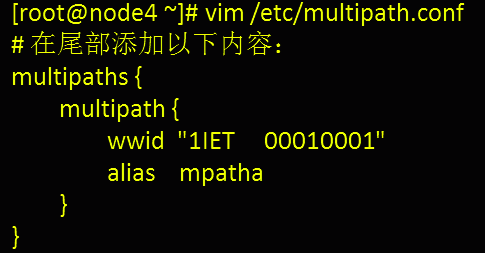
关键点就是WWID和UUID一样，即使两个设备的名称不一样但是他们的WWID一样所以是一个设备

指定获取WWID的方法

在配置文件中神明获取WWID的方法



根据得到的WWID，位多路径设备配置别名



multiupath -rr //重新加载多径

multipath -ll //查看多径信息

http、nginx、tomcat 该如何选择

Apache一个连接对应一个进程，apache非常的稳定，对php的支持简单，nginx需要配合其他后端用

Nginx可以多个进程对应一个进程，并发亮大，处理静态文件好，本身不具备动态解析的功能，需要配置其他插件或通过其他软件协同才具备动态功能。（基础并发几万）

Tomcat需要配置JDK的支持（基础并发100）tomcat更多用来做做一个应用容器，让java web app跑在里面的东西，通常用在内网和不需要流控等小型服务的场景。

访问web站点

为浏览器程序提供URL网址

URL：统一资源定位器

URI：由路径表示、着重强调与资源

URI> URL

虚拟web主机的概念：由一台服务器提供多个不同的web站点

区分方式：

基于域名的虚拟主机：域名不一样，其他相同

基于端口的虚拟主机：端口不一样，其他相同

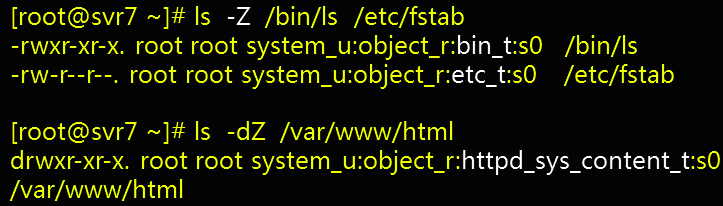
基于IP地址的虚拟主机：IP地址不一样，其他相同

多个虚拟主机，第一个虚拟化祖籍站点被视为默认站点，若客户机请求的URL不属于已知站点，则有第一个站点响应。

文件夹的权限：网页根目录的运行身份应该为apache

自定义的web目录：如果是自定义的目录就受到selinux的限制，需要修改上下文值

ls -Z 文件 查看文件的上下文值



使用chcon工具 -t：指定访问类型 -R递归修改

移动的文件，原有的上下文属性不变

复制的文件，自动继承目标文值的上下文

修改上下文值

1. chcon -R --reference=模板目录 新目录
2. 案例：有一个权限为644的文件，但是FTP无权下载



chcon -t public\_content\_t /var/ftp/rt.txt

3.a.进入到一个要同步成相同上下文值的目录 b.restorecon rt.txt

重置上下文值

使用restorecon工具

恢复为所在位置的默认上下文属性

-R，递归修改

./autorelabel 文件 下次重启后全部重置 //修改密码时用的就是这个

http的动态网站的部署：

1. 装包mod\_wsgi 2.如果有非默认端口需要semanage添加 3.修改配置时要加listen 4.可以添加一个别名WSGIScriptAlias 5.重启

交换空间：当物理内存不够时，使用磁盘来模拟内存

1.格式化交换文件系统mkswap 2.启用交换分区swapon 停用swapoff 3.开机自动启用交换分区 4.刷新swapon -a

