第一章、linux的介绍和安装

1.1 linux操作系统介绍

linux的创始人Linus torvalds。
linux与GNU和minix
linux与windows
linux与unix（POSIX标准）
linux的版本号
linux的优点

1.2 linux操作系统的安装

1.2.1 linux的常见发行版本

redhat：advanced standard 5 ； Enterprise standard 5 ；workstation standard
fedora： fedora 10
Ubuntu：ubuntu 8.10
OpenSUSE：opensuse 11.0
redflag：redflag 7
asianux: asianux 3.0

1.2.2 linux的安装过程

1、两种安装模式，以及读取信息文件
2、在时间选项中强调UTC时间和GMT时间
3、root等同administrator
4、定制安装包组，以及简述包之间的依赖关系
5、安装完成之后的gnome和KDE界面

1.3 linux操作系统的简单应用

1.3.1 linux的文本模式介绍

[root@localhost ~]
第一列root代表当前用户
第二列localhost代表主机名
第三列~代表当前所在的目录 ~家目录home目录
linux的命令可以补全 可以不全目录和文件名，如果不能补全双击tab键可以显示出要选择的命令

1.3.2 linux的登陆与登出

login 登入系统
logout 登出系统
exit 注销当前用户
clear 清屏命令

1.3.3 linux的关机

shutdown 关机命令
shutdown now 立即进入维护模式
halt 直接关机
shutdown -h now 立即关机
shutdown -r now 立即重新启动计算机
shutdown -h 20:00& 20:00 关闭计算机
shutdown -r 20:00& 20:00 重新启动计算机
shutdown -k 3 warning:system will shutdown! 只是发送消息给所以用户3分钟后进入维护模式
shutdown +3 "system will shutdown after 3 minutes!" 发送消息给所以用户3分钟后进入系统维护模式

1.3.4 linux的Init进程

Init是Linux操作系统中不可缺少的程序之一。init进程是Linux内核引导运行的，是系统中的第一个进程，其进程号（PID）永远为1。
#0 停机(千万不能把initdefault 设置为0)

#1 单用户模式
#2 多用户，没有 NFS(和级别3相似，会停止部分服务)
#3 完全多用户模式
#4 没有用到
#5 x11(Xwindow)
#6 重新启动(千万不要把initdefault 设置为6)

1.3.5 查看 linux系统信息
hostname 显示主机名
hostname eduask 修改主机名为 eduask
uname 显示系统及版本信息
-a 显示系统及版本的所有信息
-s 显示内核名称
-n 显示网络节点名称（完整的计算机名称）
-r 显示内核发行版本
-v 显示内核版本信息
-m 显示计算机类型
-o 显示操作系统的类型
--version 显示系统发行版本信息
--help 系统命令的帮助信息和参数含义

1.3.6 linux下查看用户信息
whoami 显示当前用户
who 当前系统所登陆的用户，以及所登录的控制台
w 当前系统所登陆的用户，以及所登录的控制台的详细信息

2.1.1改变目录
cd

目录的表达方法
/根目录
.当前目录
..上一级目录
~家目录

#cd/　　进入到系统根目录
#cd .　　进入当前目录
#cd ..　　进入当前目录的父目录，返回上层目录
#cd/tmp　进入指定目录/tmp
#cd ~　　进入当前用户的家目录
#cd　　进入当前用户的家目录
#cd -　　回到刚才所在的目录

2.1.2 显示当前所在目录 pwd
pwd　　显示当前所在目录的路径

2.1.3 显示文件或目录的属性 ls （dir）
#dir　　显示当前目录的内容（无颜色）
#ls　　显示当前目录的内容(有颜色)
#ls/tmp　显示指定目录/tmp的内容
#ls -l　　列出文件和文件夹的基本属性和详细信息
#ll　　列出文件和文件夹的基本属性和详细信息
#ls -a　　列出当前目录的全部内容，包括隐藏文件（在文件和文件夹前面加“.”隐藏）
#ls -l -a　列出当前目录的全部文件和文件夹的基本属性和详细信息
#ls -la　　列出当前目录的全部文件和文件夹的基本属性和详细信息
#ll -a　　列出当前目录的全部文件和文件夹的基本属性和详细信息
#ls -A　　列出当前目录的全部内容，包括隐藏文件，不显示“.”和“..”
#ls --help 列出ls命令的帮助内 容
#ls a2*　　列出以a2开头的文件和文件夹
#ls -l a2* 列出以a2开头的文件和文件夹的基本属性和详细信息

文件和文件夹（蓝色代表目录，白色代表文件，黄色代表设备文件，红色代表压缩文件，绿色代表可执行文件，浅蓝色代表链接文件）linux是以属性来控制文件是否能执行。

2.1.4 创建目录 mkdir
mkdir dir1　　在当前目录下创建dir子目录
mkdir/tmp/dir2　　在指定目录/tmp下创建dir2子目录
mkdir -p dir3/dir4　在当前目录下创建2级目录dir3和其子目录dir4
mkdir -p/dir5/dir6　在根目录下创建2级目录dir5和其子目录dir6
mkdir dir7 dir8 dir9 在当前目录下创建3个目录dir7　dir8 dir9，以空格隔开
2.1.5 创建空文本文件 touch
#touch file1　　在当前目录下创建file1文件
#touch/tmp/file2　在指定目录/tmp下创建file2文件

2.1.6复制文件命令 cp
#cp file2/tmp　　复制file2文件到/tmp目录下
#cp/tmp/file2/home　复制/tmp/file2文件到/home目录下
#cp/home/file2/tmp/file3复制/home/file2到/tmp目录下并改名为　　file3
#cp -p/tmp/file3/home　　复制/tmp/file3到/home目录下并复制文件属性
#cp -r/dir5/tmp　　复制/dir5目录到/tmp下

2.1.7移动文件或目录命令 mv
#mv file4/tmp　　移动file4文件到/tmp目录下
#mv/home/file3/tmp　　移动/home/file3文件到/tmp目录下

#mv /home/file3 /tmp/file5 移动/home/file3文件到/tmp目录下并改名为 file5
#mv file3 file4 将file3改名为 file4
#mv dir10/tmp 移动目录到/tmp下
#mv dir10 dir11 讲dir10目录改名为 dir11

2.1.8删除文件命令 rm
#rm file1 删除文件file1
#rm -f file1 不用确认直接删除file1
#rm -f file1 file2 file3 不用确认同时删除多个文件
#rm/tmp/file1 删除指定目录/tmp下的文件 file1
#rm fi* 删除以fi开头的文件
#rmdir 删除空目录
#rm -r dir 递归的方式删除非空目录dir
#rm -rf dir 不用确认直接删除非空目录dir

2.1.9 查看文件内容命令 cat
#cat/etc/passwd 查看/etc/passwd文件
#cat/etc/passwd|more 分屏查看文件内容
#cat/etc/passwd|less 分屏查看文件内容，可以上下翻页，“q”退出

2.1.10 查找文件命令 find
#find pass* 在当前目录下查找以pass开头的文件
#find/etc/pass* 在/etc目录中查找以pass开头的文件
#find/etc/pass* -print 在/etc目录中查找以pass开头的文件，并显示出来

2.1.11 在文件内容中查找关键字 grep
#grep“rpm”/etc/passwd 在/etc/passwd文件中查找关键字rpm

2.2 vi文本编辑器

2.2.1 vi的两种模式
1、命令模式 vi的默认进入状态（不可以输入字符，但可以对字符进行操作，复制，移动、删除等操作）
2、输入模式输入字符状态（只可以输入和使用del和退格backspace键删除文字）

2.2.2 vi的启动和退出
#vi file 编辑file文件
#vi/tmp/file1 编辑指定目录/tem下的 file1文件
:w 保存修改
:q 退出vi
:wq 保存并退出
:q! 强行退出vi，不保存修改

2.2.3 vi命令模式下的操作
: set nu 设置行号
: set nonu 取消设置行号

删除字符
x键或del键
7x 删掉光标后面的7个字符
dw 删除一个词（剪切）
dd 删除行（剪切）
4dd 删除4行（剪切）

复制操作
yw 复制一个词
yy 复制光标所在的行
4yy 复制光标所在行的下面 4行

粘贴操作
p 粘贴在光标所在的下一行（如果粘贴词的话，粘贴在光标字符的后面）

撤销操作
u　　撤销，可以撤销到最近的一次保存的状态
：e!　恢复到文档的初始状态

光标快速定位
G　　光标到达行末
7G　　快速找到第7行
/adm　简单搜索，快速定位光标到光标后的第一个adm单词的位置，当到行末没有的话，返回从头开始查找（类似于word的查找）

技巧
让行号永久生效
进入该用户的家目录，在目录下创建1个文件，“.vimrc”
内容 :set nu

替换内容
：7，12 s/:/?　　把第7-12行中每一行的第一个：改成？
：7，12 s/:/?/g　把第7-12行中的：全部改成？

2.2.4 进入和退出输入模式
i　　在光标之前输入文字
ESC　退出
a　　在光标之后输入文字
A　　在行尾插入文字
o　　光标下面插入1行空行
O　　在光标上面插入1行空行

3.1 文件系统

文件系统（file system）是指数据在计算机的硬盘中存放的格式，针对不同的操作系统，文件存储格式和存取的方式各不相同，所以文件系统也不尽相同。

3.1.1 windows的文件系统

1、FAT16 file allocation table 文件分配表
2、FAT32
3、NTFS new technology file system 新技术文件系统

3.2 linux文件系统介绍

1、Ext2 标准的linux文件系统
2、Ext3 Ext2的升级版，增加日志功能，并有根据日志中断重整功能。
3、linux swap linux的交换分区
4、VFAT 长文件名系统，与windows共同支持的文件系统。
其他支持的：fat、ISO9660、cramfs

3.3 linux下的目录和文件类型

在查看文件的基本属性的时候，每一行的第一位，也就是权限位之前的那一位表示文件的类型：
- 代表普通文件
d 代表目录文件
l 代表链接文件
p 代表管道文件
以及其他的s、b、c等特殊文件

文件的扩展名（后缀）
文件的后缀名主要是方便用户和系统识别，例如:“.jpg” “.mp3”用户看到可以知道.jpg是图片文件，而.mp3是音频文件；系统读取的时候可以用来识别与哪些程序关联。以方便双击打开。对系统内部来说，扩展名没有太大的意义。

3.4 linux文件系统和windows文件系统的对比

LINUX：存储设备在文件系统层次结构中，以目录表示；用正斜杠/分割目录；文件名不需要后缀；每个文件/目录都有与之相关的权限和所有权
WINDOWS：驱动器以字母表示；用反斜杠\分割目录；文件名的后缀有特殊含义；安全 特性各不相同

3.5 linux系统下的默认目录
/bin
/boot
/dev
/etc
/home
/media
/root
/sbin
/tmp
/usr
/var

3.6 linux的目录与文件的权限
3.6.1权限的类型
r 读权限 数值表示4
w 写权限 数值表示2
x 执行权限 数值表示1

4代表执行，2代表写，3代表1+2，4代表读,5代表1+4，6代表2+4，7代表1+2+4

3.6.2 三组、九位权限位

u	属主	前三位	文件的主人（文件的所有者）
g	属组	中间三位	文件主人所在的组（文件所有者所在的组）
o	其他用户	后三位	除了u和g以外的用户

3.6.3更改目录、文件的权限值
chmod 命令
1、数值表示法 chmod 数值 文件名/目录名
chmod 766 dir1 将目录dir1的权限更改为 4+2+1 4+2 4+2
chmod 777 file1将文件file1的权限更改为 4+2+1 4+2+1 4+2+1

2、字母描述法 chmod??属主(或属组或其他人或所有的)=(或者+或者-)权限 文件名/目录名
chmod u=r file1 给文件的属组赋予读取权限
chmod u=wx file1 给文件的属组赋予写和执行权限
chmod g+rw file1 给文件的属组增加读写权限
chmod g-rw file1 给文件的属组去掉读写权限
chmod o=rw file1 给文件的其他用户的权限改为读写
chmod a+rwx file1 给所有用户增加读写和执行权限

3.6.4 系统的umask值
umask值可以计算，当创建目录或文件时系统默认分配的权限。创建文件的默认权限是666减掉权限位数值，目录的默认权限是777减掉权限位的数值。
[root@localhost ~]umask
0022
查看系统默认的umask值为0022，第一位0代表粘贴位，第2-4位代表权限位
这样系统默认创建文件的权限为666-022为644为属主读写，属组读，其他读
系统默认创建文件夹的权限位777-022为属主读写执行，属组读执行，其他读执行

3.6.5
粘贴位：（sticky）当一个目录被设置为"粘着位"(用chmod a+t),则每个用户可以以完整的权限来使用和执行文件或目录，但是该目录下的文件只能由：
一、超级管理员删除
二、该目录的所有者删除
三、该文件的所有者删除

setUID 用户特殊权限位
当设置用户特殊权限位时，用户在执行这个文件时便拥有是属主的权限，便可以使用属主用户所能使用的所有系统资源。
setGID 组的特殊权限位
当设置组的特殊权限位的时候，用户在执行这个文件时便拥有文件属组的权限，便可以使用文件属组所能使用的系统资源。

用户在无特殊要求时，一般情况下，出于安全考虑，不要开启这些权限。

Suid对应数值为4
Sgid对应数值为2
t对应数值为1
特殊权限位在设置过程中占用x权限位，如果同时开启x权限，则用小写来表示，如果关闭x权限则用大写来表示。
设置举例：
chmod 1666 dir1
drw-rw-rwT root root 4096 dec 17 19:05 dir1
更改 dir1的权限，增加粘贴位权限，属主为读写，属组为读写，其他用户为读写
chmod 2666 dir1
drw-rwSrw- root root 4096 dec 17 19:05 dir1
更改 dir1的权限，增加组位特殊权限，属主为读写，属组为读写，其他用户为读写

chmod 777 dir1
drwsrwsrwt root root 4096 dec 17 19:05 dir1
更改 dir1的权限，增加粘贴位权限，用户和组位特殊权限，属主为读写执行，属组为读写执行，其他用户为读写执行

3.6.6更改目录或是文件的属主或属组
必须由文件或目录的属主或超级用户才能修改 ！！！
chown 命令更改目录或文件的属主和属组
chown u1 dir1　　将当前目录下的 dir1目录的属主改为 u1
chown u2.g1 dir1 将当前目录下的 dir2目录的属主改为 u2属组改为 g1
-R 递归式改变 指定目录及目录下所有文件和子目录
-v 显示chown命令所做的工作
可以以空格分开，同时更改多个目录或文件，并且支持通配符来修改多个文件 或目录，支持用户和组的ID来修改

chgrp 命令更改目录或文件所属的组
chgrp g1 dir2将dir2的属组更改为 g2
以空格分开，同时更改多个目录，并且支持通配符来修改多个目录和文件， 支持用户和组的ID来修改
-R 递归式改变 指定目录及目录下所有文件和子目录

4.1.1 计算机的硬件管理

在linux下，计算机所有设备是以文件的形势存在的。

在linux下查看 硬件信息

1、lspci 列出所有的PCI设备

2、fdisk -l 查看存储设备信息

3、查看/proc目录下相应的文件来查看一些设备信息

cat/proc/cpuinfo 查看 CPU的信息

4.1.2 kudzu配置硬件

kudzu 命令相当于windows的检查新硬件。

4.2磁盘管理

4.2.1 在linux下的硬盘的编号和分区的编号

1、IDE硬盘，在linux下以 hd加编号组成，由于计算机通常1个IDE通道可以连 接2块硬盘 ，所以在linux的编号如下：

第一通道上的第一块 为 hda

第一通道上的第二块 为 hdb

第二通道上的第一块 为 hdc

第二通道上的第二块 为 hdd

其他的依次类推 ，常见pc机上的IDE通道为2个

2、sata硬盘和scsi硬盘在linux下以 sd加编号组成，1个scsi通道可以连 接15块硬盘 (其中1个连 接SCSI卡)

第一通道上的第一块 为 sda

第一通道上的第二块 为 sab

其他依次类推 ，sata硬盘常应用于PC机，类似与 IDE

3、分区编号

在硬盘编号后面加上数字编号来表示第几块硬盘上 的第几 个分区

1— 4为主分区（扩展分区的编号）

5以后为逻辑磁盘 的编号

4.2.2

fdisk磁盘管理 命令

fdisk -l 显示磁盘 分区信息

对新硬盘进行分区

fdisk/dev/sdb 对第二块 scsi硬盘进行分区操作（在命令后加硬盘设备文件的名称）

如果fdisk命令不能工作可以给fdisk命令加上完整路径来执行/sbin/fdisk

fdisk实 用工具 中的命令：

a 设置和清除引导标志（相比与windows的设置为活 动的分区）

d 删除分区

n 创建分区

p 显示当前分区表

q 不保存退出fdisk实 用程序

w 保存并退出fdisk实 用程序

4.2.3磁盘 分区的格式化

mkfs命令对磁盘 进行文件系统的格式化

mkfs -t ext2/dev/sdb1将第二块 scsi硬盘的第一个分区格式化 为ext2文件系统

mkfs.ext3 /dev/sdb1 将第二块 scsi硬盘的第一个分区格式化 为ext3文件系统

mkfs.vfat /dev/sdb2 将第二块 scsi硬盘的第二个分区格式化 为vfat文件系统

4.2.4磁盘 分区的挂载

mount命令挂载磁盘 分区文件系统

mount -t ext3/dev/sdb1/media/test将ext3文件系统的第二块 scsi的第一个分区挂载到/media/test目录下

mount /dev/sdb2/media/dir将第二块 scsi的第二个分区挂载 到/media/dir目录下

-t 参数 指定文件系统类型

umount卸载　　命令
umount/media/test将挂载　　在/media/test目录下的文件系统卸载

df命令查看磁盘　　（挂载　　）信息
命令
df 不加任何参数，显示 磁盘使 用情况
* -i　显示文件系统的使用情况， 不是磁盘　的使用情况
  -h　以用户识别的方式显示磁盘　信息，以1K=1024计算
  -H　同-h，但是计算单位以1K=1000
  -l　只显示本地文件系统
  -t　加文件系统类型，只显示 指定文件系统类型
  -x　加文件系统类型，只显示 指定文件类型 意外的系统类型

4.2.4.1自动挂载　　和按需挂载

1、开机自动挂载
vi/etc/fstab　文件
增加一行
/dev/sda1　　/mnt/data　　ext3　　defaults　0 0
要挂载　　的设备　挂载　　的目录　文件系统　　操作模式
reboot　重启查看效果。

2、按需挂载
编辑2个文件/etc/auto.master（起控制作用）和/etc/auto.misc（指定挂载　　的虚拟目录和要挂载　　的设备）
vi/etc/auto.master
增加一行
/media/jake　　/etc/auto.misc　　--timeout=10
要挂载　　的真实目录　　10分钟无动作自动卸载

vi/etc/auto.misc
增加一行
rose　　-fstype=ext3　　:/dev/sda1
挂载　　的虚拟目录挂载　　的文件系统类型　要挂载　　的设备

service autofs restart　重启挂载　　服务

4.2.5 swap交换分区的调整
free 显示内存信息命令,包含物理内存，交换分区和内核缓冲区文件。
-m　以M为单位显示内存信息
1、使用虚拟设备生成空文件（将交换分区增加100M）
dd　if=/dev/zero　of=/tmp/swp1(要创建的交换分区目录) bs=10M(每个区块　的大小) count=10(区块　数量)
2、生成交换分区文件
mkswap/tmp/swp1
3、激活交换　分区
swapon/tmp/swp1
4、使交换分区永久生效，修改 配置文件
vi/etc/rc.local最后添加一行
swapon/tmp/swp1

4.2.6　创建RAID磁盘阵列
mdadm 命令
mdadm　-C　/dev/md0　　-l5　　-n3 /dev/sdb1/dev/sdb2/dev/sdb3
　　RAID设备名RAID级别　　分区数量　　分区设备名称
more/proc/mdstat　查看RAID状态
mkfs.ext3/dev/md0格式化
mount/dev/md0/media/raid挂载　　到/media/raid目录
mdadm/dev/md0　-f/dev/sdb1（损坏的设备名称）　　标记损坏设备
mdadm/dev/md0　-a/dev/sdc1（新设备名称）　　添加新设备

mdadm/dev/md0 -f/dev/sdb1（损坏的设备名称） 移除损坏的设备

4.2.7挂载使用光驱

mount/dev/cdrom/media/cd(挂载 目录)

制作ISO文件

dd if=/dev/cdrom of=/tmp/rsing.iso(iso文件名称和存放的位置)

直接使用ISO文件

mount -o loop/tmp/rsing.iso(iso文件名称和存放的位置)/media/iso(挂载 的目录)

第五章.linux下的用户和组的管理

5.1 linux系统下用户角色

在linux系统下用户的角色不同，权限和所能完成的任务也不同，用户角色是通过UID来识别的，注意：在linux下要注意root用户的UID的唯一性。

1、Root

系统管理员超级用户，系统唯一，可以登陆系统，可以操作任何文件和命令，拥有最高权限，UID值为0

2、虚拟用户

与真实 的用户分开来，这类用户不能登陆系统，但是在使用某些服务的时候使用，这类用户是系统默认添加的。

3、普通真实 用户

这类用户可以登陆系统，但是只能操作自己家目录的内容，受限账户，这类用户都是管理员自行添加的。

5.1.2 用户相关文件介绍

在windows当中可以使用计算机管理工具 中的用户和组的管理工具来对 用户进行管理，在linux下是通过对用户配置文件（区别与windows中的用户配置文件）的管理来实现对用户和组的管理

1、/etc/passwd 用户账号文件，记录所有用户记录

每行表示一个用户信息，7个字段都有各自的含义

root : x : 0 : 0 : root : /root : /bin/bash

用户名 密码 UserID GroupID 用户相关说明 用户家目录路径 用户的登陆shell

2、/etc/shadow 用户账户的影子文件，包含用户的加密密码和其他信息，两个文件互补来记录用户信息，这个文件只有root可以读取和操作

每行包含 8个字段，各项说明如下：

第1个字段 用户名

第2个字段加密口令

第3个字段上次口令改变时间， 从1970年1月1日算起的天数

第4个字段 多少天内不能改变 口令

第5个字段 多少天内必须改变 口令

第6个字段口令到期前多少天会出现警告

第7个字段 如果口令到期后几天不使用账号，则无法登陆

第8个字段 如果到这个日期不用账号则无法登陆，可以以YYYY-MM-DD格式，也可以用1970年1月1日起的天数

3、/etc/login.defs

打开这个文件对文件内容进行解释，如果修改，修改 哪些位置有哪些作用。

MAIL_DIR	邮件存放目录
PASS_MAX_DAYS	密码有效期最长时间
PASS_MIN_DAYS	密码有效期最短时间
PASS_MIN_LEN	密码最小长度
PASS_WARN_AGE	密码到期提示时间
UID_MIN	UID最小值
UID_MAX	UID最大值
GID_MIN	GID最小值
GID_MAX	GID最大值
CREATE_HOME	是否创建家目录
UMASK	UMASK值
USERGROUPS_ENAB	当删除用户后，同名组中不在存在用户的时候，是否删除该组

4、/etc/skel

存放用户启动文件的目录，类似与 windows的用户配置文件目录，为用户提供用户环境，该目录下的文件全部为隐藏文件。在添加用户时会从该目录下复制文件到用户的家目录下，相当与统一的登陆模板。

开启和关闭投影密码命令

开启用户的投影密码，使得密码得到更好的保护，不容易被别的用户得到。

该选项是一个安全选项，执行命令可以把用户名和密码分别存放在两个文件当中，影子文件就是密码文件。

pwconv 开启投影密码命令

pwunconv 关闭投影密码命令

5.1.2 用户管理

1、useradd 创建用户命令

useraddjake　创建名为jake的用户

-d指定用户的家目录

-g指定用户组

-G指定用户的附加组

-u指定用户的UID值

-p 创建密码

useradd -d/rose -g group -G root -u 505 rose 创建rose用户，指定家目录在/rose下，加入到group组，同时附加到root组，并设置UID号为505

users　查看所有登陆的用户（who）

2、tail 命令查看指定文件的末行

tail -n 3/etc/passwd　查看 passwd文件的最后三行

tail -1/etc/passwd　查看 passwd文件的最后一行

3、passwd 设置密码命令

注意：没有设置密码的用户不能使用

passwd rose 给用户rose设置密码

-d删除密码

-f 强制执行下次登陆时更改密码

-l停止账号使用

-u启用已经停止的账号

-S显示密码信息

4、userdel 删除账号命令

userdel rose　删除rose账号

userdel -r rose删除用户登陆目录及目录下的文件（类似 于windows的删除用户选择是否删除用户的文档）

5、usermod 修改 账号命令

usermod -l newname oldname

-d -g -G -u 等参数与　useradd命令参数 使用方法一样

usermod -d/home/rose -g group0 -G group1 -u 600 rose

将rose用户的家目录，主组和附加组以及UID值更改

用户的锁定与解锁

usermod -L rose锁定rose用户

usermod -U rose解除rose用户的锁定

6、gpasswd用户添加到其他组的命令

注意：只有root和组管理员能够改变组成 员

gpasswd -a u1 g1将u1加入到g1组

gpasswd -d u1 g1将u1退出g1组

gpasswd -A u1 g1将g1组的管理员指派给u1

7、id查看　ID信息命令

id rose 查看 rose用户的ID信息

5.1.3 root单用户

如果希望计算机除了root账号外其他账号不能登陆，在/etc目录中执行touch nologin，创建1个名称为 nologin的文件。如果系统只有一个人使用，可以考虑修改 /etc/inittab文件，将默认启动值改为2。

5.2 组的管理

5.2.1 组相关文件介绍

1、/etc/group

用户组的特性在系统管理中为系统管理员提供了极大的方便，但安全性也是值得关注的，如某个用户下有对系统管理有最重要的内容，最好让用户拥有独立的用户组，或者是把用户下的文件的权限设置为完全私有；另外root用户组一般不要轻易把普通用户加入进去，

/etc/group 内容具体分析

/etc/group 的内容包括用户组（Group）、用户组口令、GID及该用户组所包含的用户（User），每个用户组一条记录；格式如下：　group_name:passwd:GID:user_list

在/etc/group 中的每条记录分四个字段：

第1字段：用户组名称；

第2字段：用户组密码；
第3字段：GID
第4字段：用户列表，每个用户之间用,号分割；本字段可以为空；如果字段为空表示用户组为GID的用户名；
root : x : 0 :root,rose
root组 x是密码段 GID是0 root用户组下包括root、rose以及GID为0的其它用户（可以通过/etc/passwd查看）
2、/etc/gshadow
/etc/gshadow是/etc/group的密码文件，用户组（Group）管理密码就是存放在这个文件 。
/etc/gshadow和/etc/group是互补的两个文件；对于大型服务器，针对很多用户和组，定制一些关系结构比较复杂的权限模型，设置用户组密码是极有必要的。比如我们不想让一些非用户组成员永久拥有用户组的权限和特性，这时我们可以通过密码验证的方式来让某些用户临时拥有一些用户组特性，这时就要用到用户组密码；
/etc/gshadow格式如下，每个用户组独占一行；
groupname:password:admin,admin,...:member,member,...
第1字段：用户组
第2字段：用户组密码，这个段可以是空的或!，如果是空的或有!，表示没有密码；
第3字段：用户组管理者，这个字段也可为空，如果有多个用户组管理者，用,号分割；
第4字段：组成员，如果有多个成员，用,号分割；
jake:!::rose
rose:oUS/q7NH75RhQ::rose
第一字段：这个例子中，有两个用户组jake用rose
第二字段：用户组的密码，jake用户组无密码；rose用户组有已经，已经加密；
第三字段：用户组管理者，两者都为空；
第四字段：jake用户组所拥有的成员是rose，rose用户组有成员rose

5.2.2 组的管理
1、groupadd添加用户组
-g指定GID
-o 一般和g选项同时使用，可以与已有组的GID相同
groupadd -go 501 g1 创建组g1其GID可以与已有的组重复
2、gpasswd设置用户组的密码
一般的情况下，没有必要设置用户组的密码；
gpasswd rose 修改 rose 组的密码
3、groupdel删除用户组
groupdel g1删除g1组（没有用户的空组）
4、groupmod 修改组 属性
-g指定新的GID
-o 与-g配合使用同groupadd的-o
-n 修改组名
groupmod -g 601 g1修改 g1的GID为601
groupmod -n g11 g1将g1组改名为 g11
5、newgrp 切换用户组
newgrp root切换到root组

5.3普通用户权限提升
1、su切换用户命令
su 直接默认切换到root用户
su - root更改环境变量为root用户的
su -m root保留环境变量不变
su -c“/usr/sbin/useradd u1” root 以root的身份执行useradd命令，-c代表执行一个命令后就结束。其中命令需要输入命令文件的绝对路径。
2、sudo 命令
由于su对转换到root后，权限的无限制性，所以su并不能担任多个管理员所管理的系统。假如用su来转换到root来管理系统，也不能明确哪些工作是由哪个管理员进行的操作。特别是对于服务器的管理有多人参和管理时，最好是针对每个管理员的技术特长和管理范围，并且有针对性的下放给权限，并且约定其使用哪些工具来 完成和其相关的工作，这时我们就有必要用到 sudo。

通过sudo，我们能把某些root有针对性的下放，并且无需普通用户知道root密码，所以sudo 相对于权限无限制性的su来说，还是比较安全的，所以sudo也能被称为受限制的su ；另外sudo 是需要授权许可的，所以也被称为授权许可的su；

sudo执行命令的流程是当前用户转换到root（或其他指定转换到的用户），然后以root（或其他指定的转换到的用户）身份执行命令，执行完成后，直接退回到当前用户；而这些的前提是要通过sudo的配置文档/etc/sudoers来进行授权；

visudo来增加一行

u1 ALL=(root) NOPASSWD：/bin/cat u1用户可以转换到root下不需要输入密码执行/bin/cat命令

u1 ALL=（root）/bin/cat,/user/bin/passwd,!/user/bin/passwd root

u1 用户可以转换到root下需要输入密码执行/bin/cat,/user/bin/passwd，但不能执行/user/bin/passwd root来修改用户 密码。

执行sudo命令

sudo -l 列出用户在主机上可用的和被禁止的命令

sudo 命令（命令为绝对路径）来执行命令

sudo/bin/cat/etc/shadow

5.4磁盘配额

windows不能对组进行配额设置，而linux可以对组进行配额限制。

1、vi/etc/fstab文件

将要设置配额的分区设置开机自动挂载 在添加行在defaults后面加上，usrquota（grpquota）表示要建立用户或组的磁盘配额

2、重新挂载 文件系统

之前重启看效果，可以使用umount -a卸载 所有文件挂载 ，然后使用mount -a挂载 所有文件系统

3、在挂载 目录下创建aquota.user文件

在挂载 目录下执行touch aquota.user

通常要对该文件配置权限，防止用户随便访问。

4、进行配额检查

执行quotacheck -avu（g）（g是启用组配额）

5、设置用户磁盘配额

执行edquota -u rose

默认使用vi编辑rose用户的配额文件

filesystem	blocks	soft	hard	inodes	soft	hard
/dev/sdb1	4	0	0	1	0	0

4个数据块 和1个inodes

软极限和硬极限讲解（结合windows中的配额提醒来讲）

如果设置宽限时间，可以让用户在规定的时间内可以超过软极限，但必须在硬极限之内。

6、设置宽限时间

edquota -t编辑时间。

7、启用配额

quotaon/qt(配额目录)

8、进行配额测试

创建文件，占用磁盘空 间，然后超过软极限，看提醒，然后再超过硬极限，看效果

如果要对其他用户设置相同的配额，可以复制配额

edquota -up rose u1 u2 u3

如果要使配额每次启动生效，可以将配额检查和激活 命令放在默认/etc/rc.d/rc.sysinit启动脚本中。

6.1 linux下软件介绍

6.1.1 rpm包

Redhat Package Manager

红帽子包管理器(RPM)提供了标准化方　式，可以对各种实　用程序和应用程序组织所要的软件。红帽子包管理器使红帽子公司很容易地把Linux组织成不到两千个包，而不是几　　万个文件。

类似于windows的.exe文件

6.1.2 srpm包

srpm包为未编译过的rpm包，需要以rpm管理的方式编译，然后以rpm的安装方式安装

6.1.3 tar包

压缩包，常见的有.tar.gz和.tar.bz2，其中gz为使用gzip压缩的tar包，如“linuxqq_v1.0-preview3_i386.tar.gz”最新的QQ版本，前面为文件名称，后面为文件的扩展名，我们可以看出是以gzip压缩的tar包；.tar.bz2是以bzip压缩的tar包。

6.2 rpm包

6.2.1 rpm与cpu

rpm包是依赖cpu架构的，常见的格式：

扩展名

CPU

noarch.rpm

不依赖于CPU，　可以在所有计算机上安装

i386.rpm

基于Intel 386 CPU，这些RPM包可以在所有Intel兼容计算机上安装

i486.r pm

用于带Intel 486 CPU的计算机(随时)

i586.rpm

用于带Intel 586 CPU的计算机

i686.rpm

用于带Intel 686 CPU的计算机

ia64.rpm

用于带Intel ltanium 64位CPU的计算机

alpha.rpm

用于带HPAlpha　CPU的计算机，最初是DEC公司开发的

nthlon.rpm

基于AMDAthlon　CPU

ppc.rpm

用于带Apple Powe rPC CPU的计算机

s390.rpm

用于基于S/390 CPU的IBM服务器

sparc.rpm

用于带Sun系统公司SPARC　CPU的计算机

6.2.2 rpm软件包的查询

rpm 命令

-q对已安装的包进行简单查询

rpm -q　packagename（包的名称）

rpm -qi packagename对已安装的包进行详细信息查 询

rpm -ql packagename 查询已安装包中包含的文件

rpm -qa 显示已经安装的所有rpm包

rpm -qa|grep　linux 显示已经安装的所有包含　linux字段的包

6.2.3 rpm包的安装

rpm -i packagename 安装包（在包所在的目录下）

rpm -i/media/udisk/linux/linuxqq_v1.0-preview3_i386.rpm　安装指定目录下的包

rpm -ivh packagename 安装包并显示安装的进度和详细信息

-v 显示安装过程的详细 处理过程

-h 显示安装进度

6.3 rpm包的卸载
rpm -e packagename卸载 已安装的rpm包
可以以空格隔开同时删除多个包

举例为：
linuxqq-v1.0-preview3.i386.rpm
RealPlayerGoldforLinuxGold11.rpm
VirtualBox-2.1.0_41146_rhel5-1.i386.rpm

6.3 srpm包的安装
源代码RPM包的结尾通常是.src.rpm
使用方法
rpm -i rpmpackage.src.rpm
cd/usr/src/redhat/SPECS
rpmbuild -bb rpmpackage.specs
/usr/src/redhat/RPM/i386/目录下，有一个新的 rpm包，这个是编译好的二进制文件。
rpm -i new-package.rpm即可安装完成。

6.4 tar包软件的安装和卸载
tar 包为压缩包
常见的文件类型为.tar.g z .tar.bz2 .tgz .tar.zip
在linux下安装方式为：
1、先解压缩，各种文件类型的 解压缩方式不同
.tar.gz .tgz 文件执行
tar -xvzf softname.tar.gz
tar -xvzf softname.tgz
-x解压缩文件
-v 显示详细过程
-z支持gzip压缩文件
-f 指定压缩文件
tar -xvjf softname.tar.bz2
-j支持bzip2压缩文件
unzip -v softname.tar.zip
-v 解压文件
-d 指定解压缩目录
2、在软件所在目录下会生成同名的目录，里面会存放着所有文件，进入到这个目录
3、阅读readme文件或是install文件，查找执行配置，编译，安装命令方式
4、执行配置、编译和安装命令
通常为
./configure 执行配置
make 编译
make install 安装
make clean 清理临时文件
5、tar包的卸载
可以在安装目录下执行
make uninstall
也可以直接删除目录，文件分散多多少个目录就删除多少个目录

演示举例
linuxqq_v1.0-preview3_i386.tar.gz
VmwareToolsforlinux.iso
webmin-1.400.tar.gz
wine-1.1.11.tar.bz2

7.1 网卡 的配置
7.1.1 修改网卡 的配置文件
网卡配置文件的目录/etc/sysconfig/network-scripts
网卡 的配置文件类型
ifconfig-ethX 有线网卡 的配置文件
ifconfig-ethX:X 有线网卡 的虚拟网卡 的配置文件
ifconfig-wlanX 无线网卡 的配置文件
网卡配置文件中各项的含义
DEVICE—— 设备名
BOOTPROTO—— IP地址的获取方式(静态static或者dhcp)
HWADDR—— MAC地址
ONBOOT——开机启动
IPADDR—— Ip地址
NETMASK——子网掩码
可以使用vi编辑配置文件来配置网卡

7.1.2使用命令配置网卡
ifconfig 查看 ip信息
ifconfig eth0 200.200.200.2 netmask 255.255.255.0
配置eth0的IP信息，如果是有类的 IP地址可以省略netmask（比较rip路由协议）
ifdown eth0 禁用网卡
ifup eth0 启用网卡
ifconfig eth0 hw ether 00:11:22:33:44:55
修改网卡 eth0的MAC地址

7.1.3使用setup命令配置（文本用户接口模式）

7.2 服务管理
7.2.1 服务的查看
1、ntsysv 文本用户接口查看
使用空格键选择或是取消
2、chkconfig 命令查看开机服务启动情况
chkconfig - - list 查看所有服务开机同时的开启情况
chkconfig - - list 服务名 查看开机服务开启的情况
chkconfig - - add 服务名 设置为开机启动
chkconfig - - del 服务名 设置为开机不启动

7.2.2 服务的管理
service 服务名 start 启动服务
service 服务名 stop 停止服务
service 服务名 restart 重新启动服务
/etc/init.d/服务名 start 启动服务
/etc/init.d/服务名 stop 停止服务
/etc/init.d/服务名 restart 重新启动服务

7.2.3 查看和关闭服务进程
ps 命令
ps -A 简明查看系统启动的所有进程
ps -aux 显示所有用户所有进程的详细信息
ps -A|grep 服务名 显示指定服务的进程简明信息
ps -aux|grep 服务名 显示指定服务的详细进程信息
kill 命令
kill 进程号 关闭指定进程
killall 服务名 关闭服务的所有进程
kill -9 进程号 强制关闭指定进程
killall -9 服务名 强制关闭服务的所有进程

8.1 NFS服务器
8.1.1 NFS服务器介绍
NFS network file system 网络文件服务 器
最初由SUN公司发展起来，一种简单的文件服务器，NFS允许一个系统在网络 上与他人共享目录和文件。
8.1.2配置NFS服务器
1、NFS的配置相关文件
/etc/exports
NFS服务的管理
service nfs start(stop,restart)
检查NFS服务是否开机启动
chkconfig - - list nfs
检查NFS包是否安装
rpm -qa|grep nfs
NFS的安装
rpm -ivh/media/cdrom/RedHat/RPMS/nfs-utils-1.0.6-46.i386.rpm
rpm -ivh/media/cdrom/RedHat/RPMS/portmap-4.0-63.i386.rpm（nfs相关服务进程）

2、vi/etc/exports编辑NFS的服务器配置文件
在配置文件中以行为单位写入共享信息，格式如下：
directory client （option1，option2）
directory代表共享目录
client 代表授权主机
（）内的内容代表常用操作选项
操作选项
rw 可读写权限
ro 只读权限
all_squash 所有用户登陆都以匿名用户身份访问
anonuid 指定匿名用户的UID（默认以nobody的身份登陆）
anongid 指定匿名用户的GID（默认以nobody的身份登陆）
sync 数据同步写入硬盘
async 数据先存放在内存中，不直接写入硬盘
example：
/nfs/share*(async)
将/nfs/share共享给所有人访问，默认是只读，数据不直接写入硬盘
/nfs/sh1 192.168.1.*(ro,all_squash,async)
将/nfs/sh1目录共享给192.168.1.0网段的客户端访问，访问时以只读，匿名用户，数据不直接写入硬盘
/nfs/sh2 192.168.1.100(rw,sync,anonuid=500,anongid=500)
将/nfs/sh2目录共享给指定IP192.168.1.100，访问以UID和GID500的用户的身份登陆，读写权限，数据直接写入硬盘.

3、NFS客户端的访问
查看 NFS共享
showmount -a 在server上应用，查看已经mount上本机NFS共享目录的机器
showmount -e NFS服务器的IP地址
查看指定NFS服务器上的共享目录
mount 192.168.1.1:/nfs/sh2/mnt/nf2
将NFS服务器192.168.1.1上的/nfs/sh2共享目录挂载 到本机的/mnt/nf2目录下
如果指定文件系统类型
mount -t nfs 192.168.1.1:/nfs/sh2/mnt/nf2

8.2 samba服务器
8.2.1 samba服务器介绍
SMB协议
SMB（Server MessageBlock，服务信息块 ）协议可以看作是局域网上的共享文件/打印机的一种协议，它可以为网络内部的其 它Windows和Linux机器提供文件系统、打印服务或是其他一些信息。
samba

Samba是用来实现SMB的一种软件，由澳大利亚的Andew Tridgell开发，是一种在Linux（Unix）环境下运行的免费软件。Samba整合了SMB协议及Netbios协议，使其运做在TCP/IP上。能够让Unix based的机器与windows互动，采用的是服务器/客户端的架构，执行Samba客户端程序，我们就可以访问Windows主机上的共享资源。而运行Samba服务器，Windows主机也可以访问Linux上的共享资源。

SAMBA服务有两个进程：
smbd：SMB服务器
nmbd：netbios名字服务器。
smbd为SMB客户机，诸如Windows9x/NT等提供Windows NT和Lan Manager风格的文件和打印服务。
nmbd提供浏览支持，使采用Linux操作系统的计算机用户可以融入使用netbios协议的windows网络。

Samba服务能够做什么
1. 在网络 上共享目录，就好像一台文件服务器一样。
2. 在网络 上共享打印机。
3.决定每一个目录由谁来使用，可以让一个人、某些人、组和所有人访问。
4.决定打印机由谁来使用，可以让一个人、某些人、组和所有人使用。
可以看出，安装和配置好了Samba服务器后，Linux就可以使用Windows网络中的文件和 打印服务器了。

8.2.2图形化 界面配置samba服务器
1、访问Samba服务器配置工具
依次单击“主菜单→系统设置→服务器设置→Samba服务器”，即可打开Samba服务器配置窗口。
注意：
1.必须以root用户身份才可以对Samba服务器进行配置。
2.也可以在终端窗口输入redhat-config-samba命令打开配置窗口。
2、进行服务器设置
这里首先要对Samba服务器的基本设置和安全选项进行配置，单击配置窗口上的“首选项→服务器设置”，即可打开服务器设置对话框（图2）。
1）基本设置
在对话框的“基本”标签页，我们可以指定Linux主机所在的工作组名称，需要注意的是，此处的工作组 名称不一定非得与Windows主机所在的工作组名称一致。
2）安全设置
Samba服务器安全设置，这里一共有四个选项，分别介绍如下：
A.验证模式：如果Windows主机不是位于NT域里，此处应该选择“共享”验证模式，这样只有在连 接Samba服务器上的指定共享时才要求输入用户名、密码；
B.验证服务器：对于“共享”验证模式，无须启用此项设置；
C.加密口令：应该选择“是”，这样可以防止黑客用嗅探器截获密码明文；
D.来宾账号：当来宾用户要登录入 Samba服务器时，他们必须被映射到服务器上的某个有效用户。选择系统上的现存用户名之一作为来宾Samba账号。当用户使用来宾账号登录入Samba服务器，他们拥有和这个用户相同的权限。
3、添加共享目录
添加共享目录，单击Samba配置窗口工具栏上的“增加”按钮，即可打开一个添加共享对话框。
1）在该对话框上的“基本”标签页上，指定要共享的目录为某个存在的目录，例如可以指定/tmp，再指定该目录的基本权限是只读还是读/写。
2）在“访问”标签页上，可以指定允许所有用户访问、或者只允许某些用户访问。
4、添加samba共享用户
添加用户，在首选项中选择samba用户管理，启动Samba用户管理界面，先要选择一个linux用户，然后在这个用户下面建立windows登录时使用的用户和密码。使用这个windows用户登录时自动继承linux用户的权限，默认有linux用户的主目录的访问权限。
确定后一个新用户就建立好了，添加共享目录时就可以分配每个用户的访问目录来。
5、从Windows访问Samba服务器
须启动Samba服务。打开一个终端窗口，键入“service smb start”命令，即可出现以下提示信息，表示Samba服务已经启动：

```
# service smb start
启动SMB 服务 [确定]
启动NMB 服务 [确定]
```

8.2 文本界面下配置samba服务器

1、samba相关

后台进程：smbd，nmbd

使用端口：137，138，139

所需RPM包：samba，samba-common，samba-client

相关RPM包：samba-swat

配置文件：/etc/samba/smb.conf

samba服务的启动/停止/重启

```
service     smb     start
service     smb     stop
service     smb     restart
```

2、samba主配置文件介绍

/etc/samba/smb.conf

使用[]分成几段，每段的含义

[global]：一些全局配置

[homes]：让用户可以访问其主目录

[printers]：定义共享的打印机资源

[global段的配置

```
workgroup   配置工作组
security              安全模式，共享级别（user，share）
```

[homes]共享段的配置

example：

```
[tmp]
comment=  Temporary file space   共享描述
path=/tmp                        共享目录
read only=   no                  共享权限
browseable=   yes                是否显示（隐藏共享）
public=   yes                    公开访问，提供给所有用户
```

配置共享级别的samba

example：

```
security=   share

[share]
comment=  share test
path=/media/share
read only=   no
browseable=   yes
public=   yes
```

添加共享目录/media/share，共享名为share，描述为test，开放给所有用户访问

配置用户级别的samba

example：

```
security=   user

#smbpasswd  -ajake共享访问用户为jake
password:            共享访问密码为***
```

8.3 windows和linux下的共享互访

linux访问windows

1、使用mount

```
mount   windowsIP地址/共享名   本机目录   -o   username=用户名
```

2、mount.cifs

```
mount.cifs   windowsIP地址/共享名   本机目录   -o   username=用户名
```

3、使用mount加参数   -t cifs

```
mount   windowsIP地址/共享名   本机目录   -o   username=用户名
```

4、使用sambaclient

smbclient -L windows计地址/共享名 -U 用户名
windows访问linux
windows访问linux与访问windows相同，使用UNC路径

9.1.DHCP服务器??

1.DHCP（dynamic host configure protocol）动态主机配置协议
最大的功能就是向客户端提供TCP/IP信息，使用的是UDP:67端口
2.手动设定适合：适用小型网络
3.手动输入IP地址和自动获取比较优缺点
4.DHCP服务器的功能：
对客户机动态分配TCP/IP信息　IP地址、子网掩码、默认网关、首选DNS服务器…
安全而又可靠的设置IP地址
减轻了网络 管理员的负担
解决了网络内　　IP地址资源不足的情况
5.DCHP server
DHCP服务器按照顺序发放IP并不冲突。?
6、DHCP的分发 ：租约产生和租约更新

1、DCHPDISCOVER包	广播要IP? 全知道	请求
2、DHCPOFFER包	SERVER回应假设某台快	响应
3、DHCPREQUEST包	选择IP确认	选择
4、DHCPPACK包	广播确认给客户使用	确认

9.2 linux下的　DHCP
1、dhcp的主配置文件
/etc/dhcpd.conf
2、dhcp网卡配　　置文件
/etc/sysconfig/dhcpd
3、dhcp中继网卡配　　置文
件
/etc/sysconfig/dhcrelay
4、dhcp服务的启动/停止/重启
service　　dhcpd　　start
service　　dhcpd　　stop
service　　dhcpd　　restart

9.3/etc/dhcpd.conf
9.3.1 dhcpd.conf文件
　在redhat Enterprise linux5中，默认是空文件，配置文件存放在/usr/share/doc/dhcp-3.05/dhcpd.conf.sample
#cp/usr/share/doc/dhcp-3.05/dhcpd.conf.sample/etc/dhcpd.conf
将配置文件拷贝到/etc下，并覆盖dhcp.conf
配置文件各字段说明
subnet　X.X.X.X netmask X.X.X.X
指定dhcp服务工作网段
range
指定分配地址段
default-lease-time
默认租期（请求续租时间）
max-lease-time
最大租期
option routers
分配路由器
option domain-name
分配域名
option domain-name-servers
分配DNS server

example：

```
subnet 192.168.0.0 netmask 255.255.255.0{      设置192.168.0.0/24子网声明
          range 192.168.0.2 192.168.0.253;     设置动态地址池 192.168.0.2 192.168.0.253
          default-lease-time 21600;            设置缺省的地址租约　21600
          max-lease-time 43200;                设置客户端最长的地址租期　43200
          option domain-name “huayu.com”;  设置客户端的域名 huayu.com
```

option routers 192.168.0.254;　　设置默认网关　192.168.0.254
option domain-name-servers　192.168.0.254;　设置DNS服务器　192.168.0.254
}
Ip绑定
host
为绑定主机起名（并不是分配给对方的名字）
hardware ethernet
指定硬件地址
fixed-address
指定IP地址或主机名
支持为绑定主机单独分配其他网络数 据
example：
hostjoe{
hardware ethernet 08:00:2b:4c:29:32;指定主机的MAC地址
fixed-address 192.168.103.211;　　为指定主机分配域名
option host-name "joe";　　为绑定主机起名
}

10.1 DNS服务器介绍

DNS domain name system域名系统

1、网络中，计算机 通过IP地址来通信

IP地址记忆困难，为计算机起个好名字

域名概念的提出

DNS服务：为主机建立IP地址与域名之间的映射关系，使用域名来唯一标识网络中的计算机

2、域名称的结构

根域

顶级域：通用域、国家域、反向域

二级域

主机名称

www .sohu .com .cn? .

主机名 二级域顶级域根域

3、FQDN 完全合格的域名

主机名.主DNS后缀

4、DNS解析的过程

DNS解析不是域名，是主机名

域名查询的模式

从查询方式上分

递归查询

简单（迭代）查询

从查询内容上分

正向搜索查询

反向搜索查询

10.2 linux下的 DNS

10.2.1 DNS相关配置文件介绍

服务器端BIND

/etc/hosts

/etc/resolv.conf

配置DNS服务器地址

/etc/named.caching-nameserver.conf

DNS的主配置文件

/etc/named.rfc1912.zones

DNS的区域声明存储配置文件

/var/named

DNS数据库存放目录

/var/named/chroot/var/named

查询记录数据库存放目录

/var/named/chroot/var/named/slaves

辅助 DNS的数据库目录

10.2.2 DNS服务和安装

1、查看安装的 DNS组件

#rpm -qa|grep bind

2、安装DNS服务缺少的软件包

caching-nameserver-9.3.3-7.el5.i386.rpm

包存放的位置，在安装光盘Server目录下

3、DNS服务

service named start

service named stop

service named restart

4、配置本机的DNS服务器地址

#vi/etc/resolv.conf

nameserver 200.200.200.1

5、配置的加载

#rndc reload

10.3配置主DNS服务器

10.3.1编辑配置文件/etc/named.caching-nameserver.conf

字段解释

```
options{
          listen-on port 53{  200.200.200.1;};监听指定主机的53号端口（ipv4）
#         listen-on-v6 port 53{  ::1;};          监听指定主机的53号端口（ipv6）
          directory "/var/named";
          dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
          query-source    port 53;
          query-source-v6 port 53;
#         allow-query { localhost;};             指定允许查询的主机
};
logging{
        channel default_debug{
                file "data/named.run";
                severity dynamic;
        };
};
view localhost_resolver{
#         match-clients          { localhost;};      匹配的客户端为本机
          match-destinations{  localhost;};
          recursion yes;
          include "/etc/named.rfc1912.zones";     指定包含的区域声明文件
};
```

10.3.2 编辑配置文件/etc/named.rfc1912.zones

增加2个字段：字段含义

```
zone "baidu.com" IN{                    声明正向区域
          type master;                        定义类型为主服务 器
          file "baidu.com.zone";              指定正向数据库文件
          allow-update{  none;};              允许更新主机
};

zone "200.200.200.in-addr.arpa" IN{声明反向区域
          type master;     指定服务类型
          file "baidu.com.local";             指定反向区域文件
          allow-update{  none;};              允许更新的主机
};
```

10.3.3 进入DNS数据库目录

```
cd/var/named/chroot/var/named
```

10.3.4生成反向解析文件

```
cp  named.local baidu.com.local反向解析文件
vi baidu.com.local

$TTL       86400
@       IN      SOA     www.baidu.com.  root.www.baidu.com.   (指定主机名
                                        1997022700;   Serial
                                        28800       ;Refresh
                                        14400       ;Retry
                                        3600000     ;  Expire
                                        86400 )     ;  Minimum
        IN      NS      www.baidu.com.
1       IN      PTR     www.baidu.com.    生成反向指针记录IP为1的指向www.baidu.com
```

10.3.5生成正向解析文件

```
cp  baidu.com.local baidu.com.zone
vi baidu.com.zone

$TTL       86400
@       IN      SOA     www.baidu.com.  root.www.baidu.com.   (
                                        1997022700;   Serial
                                        28800       ;Refresh
                                        14400       ;Retry
                                        3600000     ;  Expire
                                        86400 )     ;  Minimum
        IN      NS      www.baidu.com.
www       IN      A     200.200.200.1生成主机记录A    www主机名所对应的IP地址
```

10.3.6 DNS常用记录和DNS的泛域名解析

```
A       主机记录
CNAME   别名记录
MX      邮件交换器记录
PTR     指针记录
*  别名记录可以实现泛名解析
```

10.3.7 修改数 据库文件的属主和属组

创建的文件的属组和属主为root，对named服务来说是没有权限的，需要将数据库文件的属主和属组修改为虚拟用户named

```
chown named.named baidu.com.zone
chown named.named baidu.com.local
```

10.3.8使用本机和客户端测试

host命令和nslookup命令

10.4配置DNS的简单负载均衡

在DNS的正向文件中添加一条记录

```
www   IN   A    200.200.200.1
www   IN   A    200.200.200.11
```

在DNS的反向文件中添加一条记录

```
1     IN   PTR  www.baidu.com
11     IN   PTR  www.baidu.com
```

10.5配置DNS的转发器

编辑配置文件/etc/named.caching-nameserver.conf

增加一条记录

```
options{
          listen-on port 53{  200.200.200.1;};监听指定主机的53号端口（ipv4）
    forwarders{200.200.200.2; };            添加转发DNS服务地址为200.200.200.2
#         listen-on-v6 port 53{  ::1;};          监听指定主机的53号端口（ipv6）
```

10.6配置辅助   DNS服务器

10.6.1 主DNS服务器中的配置

```
zone "baidu.com" IN{                  声明正向区域
          type master;                      定义类型为主服务 器
          file "baidu.com.zone";            指定正向数据库文件
          allow-update{  200.200.200.2;};允许更新200.200.200.2进行区域复制
};

zone "200.200.200.in-addr.arpa" IN{声明反向区域
          type master;                      指定服务类型
          file "baidu.com.local";           指定反向区域文件
```

allow-update{ 200.200.200.2;};允许更新200.200.200.2进行区域复制
};

10.6.2辅助 DNS配置
编辑配置文件/etc/named.rfc1912.zones
zone "huayu.com" IN{ 声明正向区域
type slave; 指定服务类型为 辅助
file "slaves/huayu.com.zone"; 指定正向区域文件
masters{200.200.200.2;}; 指定主DNS服务器地址
# allow-update{ none;};
};

zone "200.200.200.in-addr.arpa" IN{ 声明反响区域
type slave; 指定服务器类型为 辅助
file "slaves/huayu.com.local"; 指定反向文件
masters{200.200.200.2;}; 指定主DNS服务器地址
# allow-update{ none;};
};

第十一章Apache服务器

11.1 http 服务原理

http超文本传送协议　　80端口
https 安全的超文本传输协议　　443端口
基于C/S(客户端/服务端)模型
协议流程：
连　接：客户端与服务端建立连　接
请求：客户端向服务端发送请求
应答：服务端响应，将结果传给客户端
关闭：执行结束后关闭

11.2Apache　服务器介绍

Apache是常见的支持HTTP协议的Web服务器之一，也是使用最广泛的Web服务器。截止到今年1月，世界上大约有超过500万台　Internet服务器使用的是Apache　Server。

Apache Server的主要特点是稳定性高、速度快、功能多。通过第三方的评测，Apache Server比大多数的Web服务器都快。

Apache 服务器既是一种软件，又是一个工程。它是由千千万万的服务器代码和文档开发者共同努力的结果。在1995年4月，公开发行了第一套Apache　Server，版本号是0.6.2。Apache Server的名字来源于“A PatCHy Server”。

11.2.1Apache——A　　Patchy Server

特点：
支持最新的HTTP1.1协议。
支持PHP、CGI、Java Servlets和FastCGI。
支持安全Socket层。
集成了Perl脚本编程语言　　。
支持SSI和虚拟主机。
实现了动态共享对象　　，允许在运行时动态装载功　能模块　。
具　有安全、有效和易于扩展等特征　。

Apache的主要特点：
支持进程控制：在需要前自动复制进程，进程数量自动使用需求
支持动态加载　模块　：不需重编译就可扩展其用途
支持虚拟主机：允许使用一台　web服务器提供多个web站点的共享

11.2.2APACH E相关文件

配置文件：/etc/httpd/conf/httpd.conf
服务器的根目录：/etc/httpd
根文档目录：/var/www/html
访问日至文件：/var/log/httpd/access_log
错误日至文件：/var/log/httpd/error_log
运行Apache的用户：apache
运行Apache的组：apache
端口：80
模块存放路径　：/usr/lib/httpd/modules

11.2.3 文件系统容器和网络 空间容器

文件系统容器
<Directory>和<Files>是针对文件系统的指令。<Directory>段中的指令作用于指定的文件系统目录及其所有子目录，.htaccess 文件可以达到同样的效果。
网络 空间容器
<Location>是针对网络 空间的指令。
<Location>指令无须文件系统的支持　。
注释：对比动态站点和静态站点页面来讲解

11.2.4Apache的进程和服务

apache的进程---httpd
apache的启动 service　httpd　start

apache的停止 service httpd stop
apache的重新启动 service httpd restart

11.3 创建个人主页
11.3.1 主配置文件介绍
各字段介绍：
ServerRoot：设定Apache安装的绝对路径
TimeOut：设定服务器接收至完成的最长等待 时间
KeepAlive：设定服务器是否开启连续请求功能
MaxKeepAliveRequests：设定服务器所能接受的最大连续请求量
KeepAliveTimeout：使用者‘连续’ 请求的等待 时间上限
一般主要配置字段
1、AccessFileName
默认值：AccessFileName .htaccess
此命令是针对目录的访问控制文件的名称；
2、BindAddress
默认值：BindAddress*
设置服务器监听的IP地址；
3、DefaultType
默认值：DefaultType text/html
服务器不知道文件类型时，用缺 省值通知客户端；
4、DocumentRoot
默认值：DocumentRoot “/var/www/html/”
设置Apache提供文件服务的目录；
5、ErrorDocument
设置当有问题 发生时，Apache所做的反应；
6、<IfModule>
使用不包含在Apache安装中的模块 的命令
7、Include
包含其它的配置文件
8、Listen
默认值：所有能够连 接到服务器的IP地址
指定如何响应除去Port指定的端口地址外的地址请求；
9、Options
控制某个特定目录所能使用的服务器功能；
其值有：
None：表示只能浏览，
FollowSymLinks：允许页面连 接到别处，
ExecCGI：允许执行CGI，
MultiViews：允许看动画或是听音乐 之类的操作，
Indexes：允许服务器返回目录的格式化 列表，
Includes：允许使用SSI。这些设置可以复选。
All：则可以做任何事 ，但不包括MultiViews。
AllowOverride：加None参数表示 任何人都可以浏览该目录下的文件。
另外的参数有：FileInfo、 AuthConfig、Limit。
10、Port
默认值：Port 80
设置服务器监听的网络 端口；
11、ServerAdmin
设定管理员的电子邮件地址；
12、ServerName
设定服务器的主机名称；
13、ServerRoot
默认值：ServerRoot/etc/httpd/
设定服务器的根目录；
14、User && Group
指定服务器用来回答请求的用户ID和组ID；

11.3.2编辑主配置文件
vi/etc/http/conf/httpd.conf
第(354行)
UserDir Disable改成#UserDir Disable
(361行)启动个人主目录名称，去掉#
UserDir public_html #配置个人主目录
(369-380行)启动个人用户Web站点的访问权限，去掉#

```
<Directory/home/*/public_html>
    AllowOverride FileInfoAuthConfig  Limit
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    <Limit GET POST OPTIONS>
        Order allow,deny
        Allow from all
    </Limit>
    <LimitExcept GET POST OPTIONS>
        Order deny,allow
        Deny from all
    </LimitExcept>
</Directory>
```

11.3.3 启动或重启Apache服务
service httpd start（restart）

11.3.4 创建自己的个人主页
1、添加用户
useradd user
2、切换用户,并进入用户主目录
su - user
3、创建文档目录,建立测试页,添加执行权限
mkdir public_html 创建文档目录,
vi public_html/index.html建立测试页,
cd/home
chmod 711 user添加执行权限

11.3.5使用浏览器测试
在浏览器中http://域名或者IP地址/~用户名
example：
http://www.baidu.com/~user

11.4 发布默认站点下目录的内容
11.4.1 进入默认根文档目录并新建目录
cd/var/www/html
mkdir 目录

11.4.2 在新建的目录下生成测试文件和测试目录
touch 文件名
mkdir 目录

11.4.3编辑主配置文件
vi /etc/httpd/conf/httpd.conf
使用文件系统容器生成文件指定目录位置

```
<Directory/var/www/html/redhat>
        Options Indexes
</Directory>
```

11.4.5 重新启动服务器并测试
service httpd restart
http://www.baidu.com/redhat

11.5 配置目录访问控制

11.5.1访问控制指令

order 顺序,设定拒绝和允许的先后顺序

deny 拒绝

allow允许

example：

order deny,allow 拒绝所有的访问,除去明确允许的

“拒绝优先,即默认拒绝”

order allow,deny 允许所有的访问,除去明确拒绝的

“允许优先,即默认允许”

deny from拒绝的范围

可以是IP地址,如192.168.10.x,或者192.168.10或者192.168.1.0/255.255.255.0或者192.168.10.0/24

(针对无类的 IP地址可以加子网掩码)可以是域名,如aaa.bbb ；All代表所有的

allow from允许的范围

可以是IP地址,如192.168.10.x,或者192.168.10或者192.168.1.0/255.255.255.0或者192.168.10.0/24

可以是域名,如aaa.bbb ； All代表所有的

11.5.2对站点进行访问控制设置

编辑主配置文件

拒绝优先

```
<Directory/var/www/html/redhat>
 Options Indexes
 Order deny，allow
 Deny from all
 Allow from 200.200.200.200        只允许200.200.200.200
</Directory>
```

允许优先

```
<Directory/var/www/html/redhat>
 Options Indexes
 Order allow，deny
 Allow from all
 Deny from 200.200.200.200         只拒绝200.200.200.200
</Directory>
```

重启服务器测试

11.6配置认证指令

AuthName认证名字

AuthType认证类型 ,有两种

Basic,基本认证类型 ,所有浏览器均支持

Digest,摘 要认证类型 ,部分浏览器不支持

AuthUserFile认证用户文件,存放认证用户的列表文件

Require valid-user 授权给通过认证的所有用户

Require user 用户名授权给通过认证的指定用户

11.6.1 在主配置文件中添加授权认证的指令

```
<Directory/var/www/html/redhat>
 Options Indexes
 AuthName“rz”          认证名称为 rz
 AuthTypeBasic         认证类型为 基本认证类型
 AuthUserFile file1    指定认证用户文件
 Require valid-user    授权给通过认证的所有用户
</Directory>
```

11.6.2生成认证授权文件，并添加用户

#htpasswd -c /etc/httpd/认证文件 用户名

11.6.3更改认证授权文件的属主和属组为apache
#chown apache.apache/etc/httpd/认证文件

11.6.4 重新启动apache服务
#service httpd restart

11.6.5访问测试

11.7访问控制、认证授权的综合指令
11.7.1 两种综合情况
1、满足一种条件即可访问
Satisfy any
或者满足访问控制的条件，或者满足认证授权的条件，就可以访问指定页面、目录
2、必须同时满足2个条件才能访问
Satisfy all
必须同时满足访问控制和认证授权的条件，才可以访问指定页面、目录

11.7.2 在主文件中配置访问控制和认证授权指令
<Directory/var/www/html/redhat>
Options Indexes
Order allow，deny
Deny from all
Allow from 200.200.200.200
AuthName“rz”
AuthTypeBasic
AuthUserFile file2
Require valid-user
Satisfy all
</Directory>

11.7.3生成认证授权文件，同时添加用户
htdigest -c /etc/httpd/认证文件认证名 用户名

11.7.4更改认证文件的属主和属组为apache
chown apache.apache/etc/httpd/file2

11.7.5 重启服务并测试

11.8 分割指令
1、Include 目录/文件名.conf
apache启动时,同时加载 Include指令指定的目录下的以.conf结尾的文件，可以减少apache的主配置文件的容量
2、.htaccess 目录下的隐藏文件
可以减少apache服务的启动

11.8.1 include
在主配置文件的第209行
Include conf.d/*.conf
在指定目录中生成文件并发布
/etc/httpd/conf.d/
然后测试

11.9 .htaccess
11.9.1 在主配置文件中发布 目录,添加使用.htaccess的指令
增加一行
AllowoverrideAll

11.9.2 在指定目录下生成.htaccess文件,并添加指令
在发布　目录/var/www/html/redhat5下生成.htaccess文件
11.9.3 重新启动apache服务测试

11.10虚拟主机
11.10.1虚拟主机常用命令
1、<VirtualHost>和</VirtualHost>
用于封　装一组仅　作用于特定虚拟主机的指令。
2、NameVirtualHost
指定一个基于域名的虚拟主机将使用哪个IP地址来接受请求。
3、ServerName
设置了服务器用于辨识自己的主机名和端口号。

11.10.2配置基于端口的虚拟主机
1、编辑主配置文件，添加虚拟主机指令
```
Listen 1234
Listen 2345
<VirtualHost 200.200.200.1:1234>
        DocumentRoot/vdir/1234
</VirtualHost>
<VirtualHost 200.200.200.1:2345>
        DocumentRoot/vdir/2345
</VirtualHost>
```
2、建立虚拟主机的根文档目录，生成测试页
```
mkdir -p/vdir/1234
mkdir/vdir/2345
echo“这是端口为1234的主页！”>/vdir/1234/index.html
echo“这是端口为2345的主页！”>/vdir/2345/index.html
```
3、重新启动服务并测试

11.11配置基于IP的虚拟主机
1、添加网卡　（虚拟网卡或真实　网卡　）
2、编辑主配置文件，添加虚拟主机指令
```
<VirtualHost 200.200.200.1>
        DocumentRoot/vdir/1
</VirtualHost>
<VirtualHost 200.200.200.2>
        DocumentRoot/vdir/2
</VirtualHost>
```
3、建立虚拟主机的根文档目录，生成测试页
```
mkdir/vdir/1
mkdir/vdir/2
echo“这是端口为1的主页！”>/vdir/1/index.html
echo“这是端口为2的主页！”>/vdir/2/index.html
```
4、重新启动服务并测试

11.12配置基于域名的虚拟主机
配置基于域名的虚拟主机必须需要DNS的支持
1、配置DNS
2、在主配置文件中，添加虚拟主机指令
```
NameVirtualHost 200.200.200.1
<VirtualHost 200.200.200.1>
     ServerName www.huayu.com
     DocumentRoot/vdir/huayu
</VirtualHost>
<VirtualHost 200.200.200.1>
     ServerName www.eduask.com
     DocumentRoot/vdir/eduask
```

</VirtualHost>
<VirtualHost 200.200.200.1>
ServerName www.baidu.com
DocumentRoot/vdir/baidu
</VirtualHost>
3、建立虚拟主机的根文档目录，生成测试页
mkdir/vdir/huayu
mkdir/vdir/eduask
mkdir/vdir/baidu
echo“这是端口为huayu的主页！”>/vdir/huayu/index.html
echo“这是端口为eduask的主页！”>/vdir/eduask/index.html
echo“这是端口为baidu的主页！”>/vdir/baidu/index.html
4、重新启动服务并测试

11.13配置后台更新-WebDav
1、发布　目录
2、在主配置文件中添加认证授权指令同时添加Dav指令
<Directory/var/www/html/redhat6>
Options Indexes
Dav on
AuthName“dav”
AuthTypeBasic
AuthUserFile file3
<LimitExcept GET OPTIONS>
Require valid-user
</LimitExcept>
</Directory>
3、配置认证授权的相关文件
生成认证授权文件，并添加用户
#htpasswd　-c/etc/httpd/认证文件　　用户名
更改认证授权文件的属主和属组为apache
#chown apache.apache/etc/httpd/认证文件
4、重启服务测试
5、在服务器端给更新目录添加写的权限
chmod o+w/var/www/html/redhat6
更新测试

14.1 Mail服务器的组成
1、电子邮局
2、电子邮件发送和接收系统
3、MUA（邮件用户代理）和MTA（邮件传输代理）

14.2 Mail系统相关协议
1、SMTP协议 简单邮件传输协议
SMTP协议使用25端口
SMTP(Simple Mail Transfer Protocol)即简单邮件传输协议,它是一组用于由源地址到目的地址传送邮件的规则,由它来控制信件的中转方式。SMTP协议属于TCP / IP协议族,它帮助 每台计算机在发送或中转信件时找到下一个目的地。通过SMTP协议所指定的服务器,我们就可以把E－ mail寄 到收信人的服务器上了,整个过程只要几 分钟。SMTP服务器则是遵循 SMTP协议的发送邮件服务器，用来发送或中转你 发出的电子邮件。
2、POP 协议邮局协议
POP3协议使用110端口
POP3协议适用于不能时时在线的邮件用户。支持客户在服务器上租用信箱 ，然后利用POP3协议向服务器请求下载 ，基于TCP/IP协议与客户端/服务端模型，POP3 的认证与邮件传送都采用明文
3、IMAP协议 Internet邮件访问协议
IMAP协议使用143端口
另一种从邮件服务器上获取邮件的协议，与POP3相比，支持在下载邮件前先行下载邮件头以预览邮件的主题来源，基于TCP/IP

POP协议和IMAP协议的区别
IMAP提供摘 要预览的功能，可以使用户很方便的删除垃圾 邮件，而不把垃圾 邮件下载 到本地。

14.3 sendmail和IMAP包的检查与安装
1、rpm -qa|grep sendmail
2、rpm -qa|grep imap
3、rpm -qa|grep pop

14.4 Mail服务器相关文件
1、mail服务器的主目录
/etc/mail
2、mail服务器的主配置文件
/etc/mail/sendmail.cf
3、mail服务器的客户端文件
/etc/dovecot.conf
4、邮件服务器的启动/停止/重启
service sendmail start
service sendmail stop
service sendmail restart

14.5编辑主配置文件/etc/mail/sendmail.cf
vi/etc/mail/sendmail.cf
将第265行的注释去掉
DaemonPortOptions=Port=smtp，addr=0.0.0.0，Name=MTA
启用邮件服务器功能
默认情况下，sendmail 服务器只侦听本地的连 接，将addr字段修改为 0.0.0.0

14.6编辑/etc/mail/local-host-names
对于服务器来说，要配置主机列表，来确定需要接收哪些邮件，不存在与列表中的主机名，将会拒绝接收。

14.7访问控制设置（/etc/mail/access）
access访问控制数 据库用于定义接受或拒绝的邮件来源：
1、格式：
IP/域名 设定值
2、设定值：

OK-接收email，即便被其它规则拒绝了
RELAY允许通过该邮件主机relay的域。relay意味着OK
REJECT拒绝email并显示内部通用的错误提示
DISCARD 安静地接收随后取消掉这封邮件
example：
huayu.comRELAY允许为huayu.com的所有计算机中继邮件
200.200.200.0RELAY允许为200.200.200.0这个子网的所有机器中继邮件
3、配置好访问控制数 据库文件后需要执行命令编译生成配置文件
cd/etc/mail
makemap hash access.db<access
service sendmail restart

14.8配置Mail服务器的客户端
1、编辑客户端配置文件/etc/dovecot.conf允许POP3 IMAP 等协议
vi/etc/dovecot.conf
第17行
protocols= imap imaps pop3 pop3s
2、重新启动客户端服务
service dovecot restart

14.9 进行Mail服务器的简单测试
1、使用mail命令进行邮件编写
格式：mailjake@huayu.com
subject：邮件主题
编写邮件内容
使用
.
Cc:
来结束退出并发送
2、使用mail命令来查收邮件
mail -ujake 接收jake用户的邮件
列出邮件列表
使用编号来显示邮件内容
使用exit退出

14.10配置Mail服务的web界面
配置openwebmail作为Mail服务器的web界面
14.10.1 安装openwebmail及其组件
openwebmail及其组件不在系统安装光盘中
rpm -ivh perl-Text-Iconv-1.4.2el4.rf.i386.rpm
rpm -ivh perl-suidperl-5.8.8-10.i386.rpm
rpm -ivh openwebmail2.52-1.rpm

14.10.2配置Openwebmail
cd/var/www/cgi-bin/openwebmai/
1、vi etc/defaults/dbm.conf
将第30 -   31行修改为
dbm_ext .db
dbmopen_ext .db
dbmopen_haslock yes
2、openwebmail的初始化
./openwebmail-tool.pl -   init
3、添加openwebmail的域名服务器的和smtp服务器地址
vi etc/defaults/openwebmail.conf
第26和第27行
domainnames www.huayu.com
smtpserver 200.200.200.1

4、更改语言 和图标

vi etc/defaults/openwebmail.conf
第273行
default_languagezh_CN.GB2312
第29 4行
default_iconset Cool3D.Chinese.Simplified

vi etc/openwebmail.conf
第62行
default_languagezh_CN.GB2312
第85行
default_iconset Cool3D.Chinese.Simplified

14.10.3配置apache
配置apache简化　用户登录网址内容
vi/etc/httpd/conf/httpd.conf
第264行
ServerName www.huayu.com：80
最后添加
Alias/data/var/www/data
ScriptAlias/cgi-bin/var/www/cgi-bin
ScriptAlias//var/www/cgi-bin/openwebmail/openwebmail.pl

重新启动服务
service sendmail restart
service httpd restart
使用web界面进行收发邮件测试

15.1 FTP

15.1.1 FTP协议

FTP（File Transfer Protocol），是文件传输协议的简称。用于Internet上的控制文件的双向传输。同时，它也是一个应用程序（Application）。用户可以通过它把自己的PC机与世界各地所有运行FTP协议的服务器相连 ，访问服务器上的大量程序和信息。

在FTP的使用当中，用户经常遇 到两个概念："下载 "（Download）和"上载 "（Upload）。"下载 "文件就是从远程主机拷贝文件至自己的计算机上；"上载 "文件就是将文件从自己的计算机中拷贝至远程主机上。用Internet语言 来说，用户可通过客户机程序向（从）远程主机上载 （下载 ）文件。

TCP/IP协议中，FTP标准命令TCP端口号为21，Port方式数据端口为20。FTP协议的任务是从一台计算机将文件传送到另一台计算机，它与这两台计算机所处的位置、联接的方式、甚至 是是否使用相同的操作系统无关。假设两台计算机通过ftp协议对话，并且能访问Internet，你 可以用ftp命令来传输文件。每种操作系统使用上有某一些细微差 别，但是每种协议基本的命令结构是相同的。

15.1.2 FTP协议的传输方式

FTP的传输有两种方式：ASCII传输模式和二进制数据传输模式。

1. ASCII传输方式：假定用户正在拷贝的文件包含的简单ASCII码文本，如果在远程机器上运行的不是UNIX，当文件传输时ftp通常会自动地调整文件的内容以便于把文件解释成另外那台计算机存储文本文件的格式。

但是常常有这样的情况，用户正在传输的文件包含的不是文本文件，它们可能是程序，数据库，字处理文件或者压缩文件（尽管字处理文件包含的大部分是文本，其中也包含有指示页尺寸 ，字库等信息的非打印字符）。在拷贝任何非文本文件之前，用binary 命令告诉 ftp逐字拷贝，不要对这些文件进行处理，这也是下面要讲的二进制传输。

2. 二进制传输模式：在二进制传输中，保存文件的位序，以便原始和拷贝的是逐位一一对应的。即使目的地机器上包含位序列的文件是没意义的。例如，macintosh以二进制方式传送可执行文件到Windows系统，在对方系统上，此文件不能执行。

如果你 在ASCII方式下传输二进制文件，即使不需要也仍 会转译。这会使传输稍微 变慢 ，也会损坏数据，使文件变得不能用。（在大多数计算机上，ASCII方式一般假设每一字符的第一有效位无意义，因 为ASCII字符组合不使用它。如果你传输二进制文件，所有的位都是重要的。）如果你知道这两台机器是同样的，则二进制方式对文本文件和数据文件都是有效的。

15.1.3 Ftp 命令

1、FTP服务器的登陆
匿名用户：FTP口令：FTP
用户 ：ANONYMOUS口令：任何电子邮件
2、显示文件信息：DIR/IS
3、下载 文件：GET 文件名 （下载 到当前目录）
4、上传文件：PUT 文件名
5、多文件下载：MPUTMGET
6、
7、退出：BYE
8、帮助： HELP

15.2 linux下的相关文件和服务
1、vsftpd包的安装
vsftpd-2.0.5-10.el5.386.rpm
2、vsftpd服务名称 vsftpd
3、相关文件
/etc/vsftpd/vsftpd.conf vsftpd 的主配置文件
/etc/vsftpd.user_list 用户登录配置文件
/etc/vsftpd.ftpusers该文件中的用户绝对不能登录到主机
/etc/vsftpd.chroot_list 用户被限制其家目录，不允许向上级目录查看，默认情况下该文件并没有建立
/var/ftp匿名ftp账户的家目录
15.3 vsftpd主配置文件的参数介绍
/etc/vsftpd/vsftpd.conf文件的相关参数如下:
anonymous_enable=YES 是否允许匿名ftp,如否则选择NO
local_enable=YES 是否允许本地用户登录
local_umask=022默认的umask码

anon_upload_enable=YES 是否允许匿名ftp用户访问
anon_upload_enable=YES 是否允许匿名上传文件
anon_mkdir_write_enable=YES 是否允许匿名用户有创建目录的权利
dirmessage_enable=YES 是否显示目录说明文件,默认是YES但需要手工创建.message文件
xferlog_enable=YES 是否记录ftp传输过程
connect_from_port_20=YES 是否确信端口传输来自20(ftp-data)
chown_username=username 是否改变 上传文件的属主,如果是需要输入一个系统用户名,你 可以把上传的文件都改成 root属主
xferlog_file=/var/log/vsftpd.log ftp传输日志的路径和名字默认是/var/log/vsftpd.log
xferlog_std_format=YES 是否使用标准的ftp xferlog模式
idle_session_timeout=600 设置默认的断开不活跃 session的时间
data_connection_timeout=120 设置数据传输超时时间
ascii_upload_enable=YES ascii_download_enable=YES 是否使用ascii码方式上传和下载 文件
ftpd_banner=Welcome to chenlf FTP service. 定制欢迎 信息

15.4配置匿名的ftp服务器
15.4.1基本的匿名ftp服务器
启动vsftpd服务即可使用
使用命令行和浏览器进行测试

15.4.2配置允许匿名用户上传的ftp服务器
1、在匿名用户的主目录下，给默认的pub目录添加写权限
2、编辑ftp的主配置文件，添加允许上传语句 第27行和31行分别定义允许匿名用户上传文件和上传目录
write_enable=YES
local_umask=022
anon_upload_enable=YES
anon_mkdir_write_enable=YES
3、重新启动服务

15.4.3配置匿名用户的完全权限
在用户可以上传的基础上，对匿名用户开放所有权限，如续传，删除等，然后重新启动服务即可。
anon_world_readable_only=NO
anon_other_write_enable=YES

15.4.4配置基于端口的匿名虚拟ftp服务器
1、生成虚拟的ftp服务器主配置文件
cp/etc/vsftpd/vsftpd.conf/etc/vsftpd/port.conf
2、编辑虚拟的ftp主配置文件/etc/vsftpd/port.conf
vi/etc/vsftpd/port.conf
添加虚拟服务器的端口和匿名用户
listen_port=2121
ftp_username=ftpguest
3、创建虚拟ftp服务器的匿名用户和登录的主目录
useradd -d/var/port ftpguest
4、重新启动vsftpd服务

15.5配置本地用户的ftp服务器
需要使用用户和密码来访问的ftp服务器
1、编辑主配置文件/etc/vsftpd/vsftpd.conf，第97行，锁定所有用户的主目录
chroot_local_user=YES
2、重新启动服务

对用户限制下载速度
1、编辑主配置文件
anon_max_rate=50000
local_max_rate=200000
单位为byte/s
2、重新启动服务即可

18. iptables防火墙

18.1防火墙

1、防火墙　　的定义

所谓防火墙 指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专　　用网与公共网之间的界面上构造　的保护屏障　.是一种获取安全性方法的形象说法，它是一种计算机硬件和软件的结合，使Internet与Intranet之间建立起一个安全网关（Security　Gateway），从而保护内部网免受非法用户的侵　　入，防火墙　主要由服务访问规则、验证工具　、包过滤　和应用网关　4个部分组成，

　　防火墙 就是一个位于计算机和它所连 接的网络之间的 软件或硬件(其中硬件防火墙　　用的较少，例如国防部以及大型机房　　等地才用,因　为它价格昂贵　　)。该计算机流入流出的所有网络 通信均要经过此防火墙

2、 防火墙　　的功能

防火墙 对流经它的网络 通信进行扫描，这样能够过滤掉一些攻　　击，以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口。而且它还能禁止特定端口的流出通信，封锁特洛伊木马　　。最后，它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

3、以设备划　分防火墙　　的种类

1):软件防火墙

　软件防火墙 就是保护计算机的一套软件，装在计算机里面，以提供保护计算机的功能。如用Linux主机架设一个防火墙

2):硬件防火墙

硬件防火墙　　主要是由厂商　　设计好的硬件，里面有自己的操作系统，以提供封　包过滤　机制，故性能较佳

4、 以技术划　分防火墙

1):包过滤　型

　主要依据是网络中的分包 传输技术。包过滤技术的优点是简单实　　用，实现成本较低

2):网络 地址转换

　将封　　包中的来源或者目的IP进行更改，可以使私有网络 连上互连　　网

3):代理性防火墙

可以代理客户端将需要的资料　进行查找并返回给客户端，安全性较高，但是性能要求较高

4):监测型防火墙

可以对各个网络 层进行主动的数据分析，安全性极高，但性能要求很高

5、Linux下的防火墙 软件

　Linux防火墙　　直接由内核进行处理，安全性高，不同的Linux内核使用的防火墙　　机制

内核版本使用的软件

2.0 ipfwadm

2.2 ipchains

2.4 与 2.6 iptables

18.2 iptables

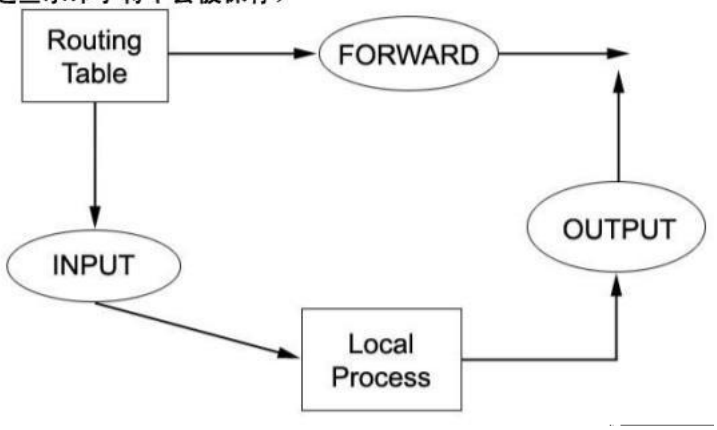
1、iptables介绍

iptables 是建立在 netfilter架构基础上的一个包过滤管理工具　　。

用户通过/sbin/iptables　命令来管理 iptables，和 route 命令相同，iptables 命令的效果在重新启动以后就不再有效。

可以使用/etc/rc.d/init.d/iptables　save将当前　iptables规则写到/etc/sysconfig/iptables　文件中，那么每次开机时/etc/rc.d/init.d/iptables start 命令会使/etc/sysconfig/iptables　中的规则生效。

2、iptables防火墙 框架图



3、表
iptables是由几张　　表所组成，每张　表又由几条链组成，每张　　表负责　不同的封　包处理机制，每条链负责不
同的封　包走向，具体采取的策略由链里的规则设定
filter表：用于过滤封　　包
Nat表：用于做地址转换
mangle表：允许改变包的内 容来进一步矫正包
4、链
INPUT链：存在于filter表，主要用于处理进入本机的封　　包
OUTPUT链：存在于filter表,主要用于处理离开本机的封　　包
FORWARD链:存在于fileter表，主要用于处理穿　　过本机的封　包
PREROUTING链:存在于nat表，主要用于修改目的 地址(DNAT)
POSTROUTING链:存在于nat表，主要用于修改 来源地址(SNAT)

18.3 iptebles文件
1、防火墙 配置保存文件
/etc/sysconfig/iptables
2、防火墙 配置保存命令
service iptables save
3、防火墙　　的启动/停止/重启
service iptables start
service iptables stot
service iptables restart
18.4 iptables的配置
1、iptables的标准语法
iptables [-t table] 命令 [chain] [rules] [-j target]
table——指　　定表名
NAT 和一般的 mangle 用 -t 参数 指定要操作哪个表。filter 是默认的表，如果没有 -t 参数， 就默认对 filter 表操作。
命令——对链　　的操作命令
chain——链　　名
rules——规则
target——动作如何进行
example:
iptables -A INPUT -p icmp -j DROP
设置INPUT规则，将所有基于icmp协议的数据包全部丢弃

2、对链的操作
-L 列出当前的iptables的规则
-vnL 列出所有iptables相关规则的详细参数
-A追加一条规则（默认添加道最后）
iptables -A INPUT -s 200.200.200.200 -j DROP
追加一条INPUT记录，将源目的地址为200.200.200.200的数据包丢弃
-I插入一条规则

iptables -I INPUT 1 -s 200.200.200.200 -j DROP
插入一条INPUT记录，将源目的地址为200.200.200.200的数据包丢弃
-D删除一条规则
iptables -D INPUT 1
iptables -D INPUT -s 200.200.200.200 -j DROP
-P 设置某条链的默认规则
iptables -P OUTPUT DROP
设置所有发送的数据包丢弃
-F 清空规则
iptables -F
清空所有iptables规则

3、操作命令
按网络接 口匹配
-i eth0匹配数据进入的网络 端口
-o eth0匹配数据流出的网络 端口
按来源目的地址匹配
-s ip匹配来源IP
-d ip匹配目的IP
example：
iptables -A INPUT -i eth0 - s 200.200.200.200 - j DROP
在INPUT链里追加一条规则，所有从eth0口进入的源地址为200.200.200.200的数据包全部丢弃

按协议匹配
协议可以是TCP,UDP,ICMP，也可以不加
example：
iptables - A INPUT -p tcp -s 200.200.200.200 -jACCEPT
在INPUT链里追加一条规则，所有源地址为200.200.200.200的基于tcp协议的数据包允许通过
按来源目的端口匹配
--sport来源端口
--dport 目的端口
example：
iptables -A INPUT -p tcp -sport 21 -j DROP
在INPUT链里追加一条规则，所有基于TCP的源端口为21号端口的数据包，全部丢弃 。

动作处理
-jACCEPT允许封 包通过而不拦截
-j DROP 不允许封 包通过

指定碎片
在TCP/IP通讯 中，每个网络接 口都有一个最大的传输单元 （MTU），用来定义了通过数据包大小的最大范围，如果数据大于MTU时，系统会将大数据包分割成多个小数据包来传输（我们把这些包称为 IP碎片），接收方再对数据进行重组，来还原整个包。
在进行包过滤 的时候，IP碎片会导致一个问题 ，第一个数据包会包含完整的包 头信息，而后续的数据包只有部分包头信息，当存在这样一条规则的时候
iptables -A FORWARD -p tcp -s 200.200.200.200/24 -d 200.200.200.1 - dport 80 -jACCEPT
iptables -P FORWARD DROP
系统会把第一个以后的包过滤掉
我们可以添加一条规则来解决这个问题
iptables -A FORWARD -f -s 200.200.200.200/24 -d 200.200.200.1 -jACCEPT

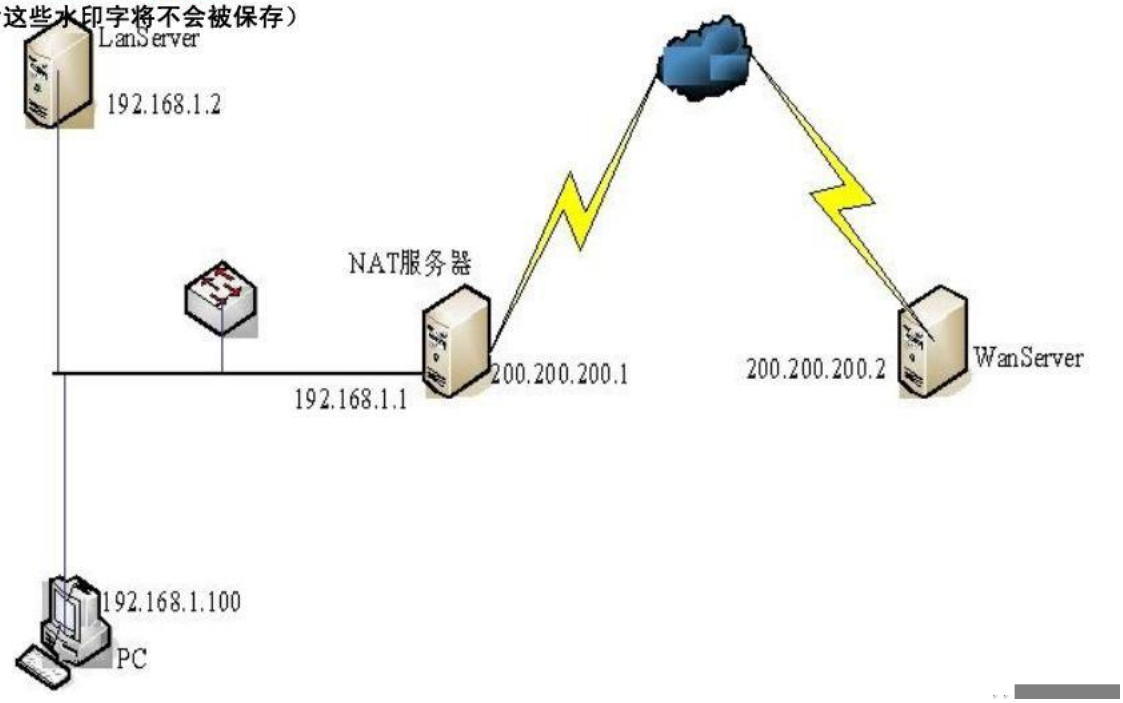
指定非
在某些选项前加上！来表示非指定值
example： -s -！200.200.200.1/24 代表除200.200.200.1以外的IP地址
-p -！icmp 代表除了icmp以外的协议。

18.5防火墙 配置
service iptables restart

重新启动iptables服务
iptables -F
清除规则
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
改变 默认规则策略
iptables -A INPUT -p tcp -s 0/0 - -dport ssh -jACCEPT
iptables -A OUTPUT -p tcp --sport ssh -jACCEPT
允许ssh
iptables -A INPUT -p udp -s 0/0 - -dport 53 -jACCEPT
iptables -A OUTPUT -p udp -d 0/0 - -sport 53 -jACCEPT
允许DNS
iptables -A INPUT -p tcp -s 0/0 - -dport 80 -jACCEPT
iptables -A INPUT -p tcp -s 0/0 - -dport 443 -jACCEPT
iptables -A OUTPUT -p tcp -d 0/0 - -sport 80 -jACCEPT
iptables -A OUTPUT -p tcp -d 0/0 - -sport 443 -jACCEPT
允许www服务

18.6 NAT表配置
1、NA T的定义
NAT英 文全称是 NetworkAddress Translation，称是网络 地址转换，它是一个IETF标准，允许一个机构以一个地址出现在Internet上。NAT将每个局域网节点的 地址转换成一个IP地址，反之亦然。它也可以应用到防火墙 技术里，把个别IP地址隐藏起来不被外界发现，使外界无法直接访问内部网络设 备，同时，它还帮助网络可以 超越地址的限制，合理地安排 网络中的 公有Internet地址和私有IP地址的使用。
2、NA T的类型
静态NAT(Static NAT)
静态NAT设置起来最为简单和最容易实现的一种，内部网络中的 每个主机都被永久映射成外部网络中的 某个合法的地址。
动态地址NAT(Pooled NAT)
动态地址NAT是在外部网络中定义 了一系列的合法地址，采用动态分配的方法映射到内部网络。动 态地址NAT只是转换IP地址，它为每一个内部的IP地址分配一个临时的外部IP地址，主要应用于拨 号，对于频繁 的远程联接也可以采用动态NAT。
网络 地址端口转换NAPT（Port一 Level NAT）
NAPT是把内部地址映射到外部网络的一个 IP地址的不同端口上。
最熟悉 的一种转换方式。NAPT普遍 应用于接入设备中，它可以将中小型的网络 隐藏在一个合法的IP地址后面。NAPT与动态地址NAT不同，它将内部连 接映射到外部网络中的一个单 独的IP地址上，同时在该地址上加上一个由NAT设备选定的TCP端口号。
3、对于POSTROUTING的目标动作
-j SNAT - to IP1[-IP2] : [port1][-port2]
IP1-IP2,指定IP地址范围
port1-port2,指定端口范围
例如:
iptables - t nat -A POSTROUTING -o eth0 -j SNAT --to 202.106.0.20
4、对于PREROUTING的目标动作
-j DNAT - to IP1[-IP2] : [port1][-port2]
IP1-IP2,指定IP地址范围
port1-port2,指定端口范围
例如:
iptables - t nat -A POSTROUTING -d 202.106.0.20 -j DNAT --to 192.168.10.239

5、NAT+防火墙 配置案例



eth0=192.168.1.1 eth1=200.200.200.1

echo 1>/proc/sys/net/ipv4/ip_forward
打开IP转发功能
service iptables restart
iptables -F
iptables -P INPUTACCEPT
iptables -P OUTPUTACCEPT
iptables -P FORWARDACCEPT
配置默认规则策略
iptables -t nat -A POSTROUTING -o eth0 -j SNAT - -to 200.200.200.1
配置企业 内部上网，将内网的 IP地址伪 装成200.200.200.1
iptables -t nat -A PREROUTING -p tcp -d 200.200.200.1 - -dport 80 -j DNAT --to
192.168.1.2:80
做端口映射，将192.168.1.2：80映射成公网 200.200.200.1
iptables -t nat -A PREROUTING -p tcp -d 200.200.200.1 --dport 443 -j DNAT --to
192.168.1.2.443
做端口映射，将192.168.1.2：443映射成公网 200.200.200.1
iptables -A INPUT -p icmp -s 0/0 -jACCEPT
iptables -A OUTPUT -p icmp -d 0/0 -jACCEPT
允许ping
iptables -A FORWARD -p tcp -s 0/0 -d 192.168.1.2 - -dport 80 -jACCEPT
iptables -A FORWARD -p tcp -s 0/0 -d 192.168.1.2 - -dport 443 -jACCEPT
设置转发规则，允许外网访问内网的 www服务
service iptables save
保存配置